Πανεπιστήμιο Θεσσαλίας
Πολυτεχνική Σχολή
Τμήμα Μηχανικών Ηλεκτρονικών Υπολογιστών,
Τηλεπικοινωνιών και Δικτύων

Διπλωματική Εργασία

Υποστήριξη ασφαλούς συνεργασίας ανάμεσα σε προσωπικές συσκευές διαφορετικών χρηστών - επέκταση του συστήματος OmniStore

από

Αντώνης Γκογκάκης

Επιβλέποντες:

- Σπυρίδων - Γεράσιμος Λάλης
- Δημήτριος Κατσαρος

Βόλος, 2008

Στην οικογένεια μου.

Περιεχόμενα

Ευχαριστίες

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή μου Σπύρο Λάλη για την πολύτιμη βοήθεια του, αλλά κυρίως για την εμπιστοσύνη που μου έδειξε. Επιπλέον θα ήθελα να ευχαριστήσω τους φίλους και συμφοιτητές μου Άγγελο-Χρήστο Αναδιώτη, Νίκο Παπαβασιλείου για την ψυχολογική τους υποστήριξη κατά την διάρκεια συγγραφής του κώδικα. Τέλος είμαι ευγνώμων στους γονείς μου για την υποστήριξη τους σε όλα μου τα εγχειρήματα.

πρόλογος

Είναι γεγονός ότι η χρήση κινητών συσκευών με ικανότητα δικτύωσης αυξάνεται ραγδαία. Οι κινητές συσκευές συνεργάζονται μεταξύ τους, δημιουργώντας δίκτυα συσκευών. Κυριότερο πρόβλημα στα παραπάνω δίκτυα είναι η μη εξουσιοδοτημένη χρήση κάποιας συσκευής. Δημιουργείται λοιπόν το πρόβλημα της ασφαλούς συνεργασίας κινητών συσκευών. Στην παρούσα διπλωματική εργασία σχεδιάστηκε και υλοποιήθηκε μια λύση στο πρόβλημα της ασφαλούς συνεργασίας προσωπικών συσκευών διαφορετικών χρήστών. Βασιστήκαμε στο σύστημα OmniStore, ένα σύστημα διαχείρισης αρχείων που αποτελείται από κινητές συσκευές και υπηρεσίες υποδομής. Η εργασία είναι δομημένη ως εξής: αρχικά γίνεται μια σύντομη παρουσίαση του συστήματος OmniStore, ακολουθεί περιγραφή των απαιτήσεων ασφαλούς συνεργασίας σε δίκτυα κινητών συσκευών και στη συνεχεια περιγραφή και αξιολόγηση της προσέγγισης μας. Τέλος γίνεται μια παρουσίαση διαφόρων εργασιών που προσπαθούν να δώσουν λύση στο πρόβλημα της ασφαλούς συνεργασίας συσκευών.

Κεφάλαιο 1

Το σύστημα OmniStore

1.1 Εισαγωγή

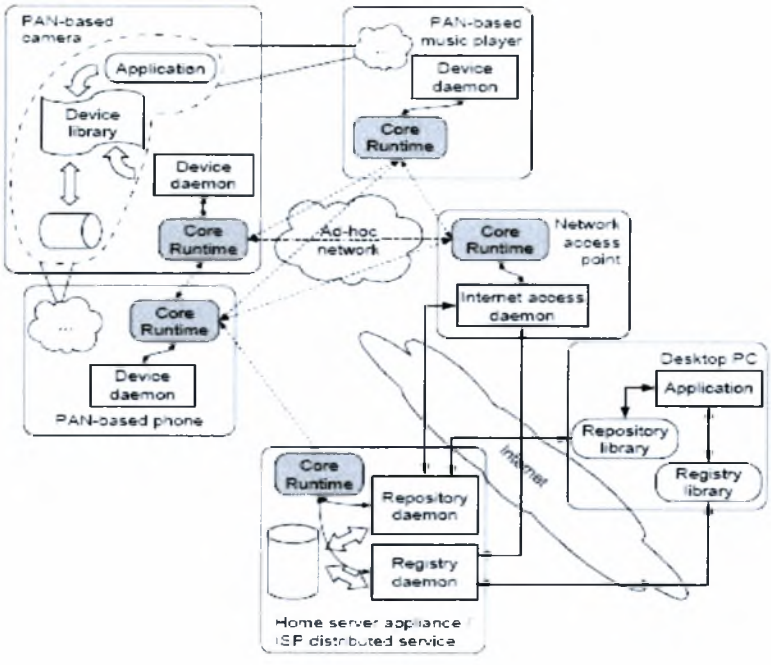
Το OmniStore [3] είναι ένα σύστημα διαχείρισης δεδομένων που παράγονται απο κινητές συσκευές, οι οποίες αποτελούν το προσωπικό δίκτυο συσκευών (Personal Area Network) του χρήστη. Η αποθήκευση δεδομένων γίνεται στις ίδιες τις συσκευές και σε σταθερή αποθήκη (repository), ενώ παράλληλα υποστηρίζεται αυτοματοποιημένη και ασύγχρονη ροή δεδομένων μεταξύ προσωπικού δικτύου συσκευών και σταθερής αποθήκης.

1.2 Αρχιτεκτονική Συστήματος

Το σύστημα αποτελείται απο τα παρακάτω στοιχεία

- Δαίμονας κινητής συσκευής (portable device daemon) και βιβλιοθήκη κινητής συσκευής (device library)
- Μητρώο συσκευών (device registry) και βιβλιοθήκη μητρώου (registry library)
- Αποθήκη δεδομένων (data repository) και βιβλιοθήκη αποθήκης δεδομένων (data repository library)
- Πύλες πρόσβασης διαδικτύου (internet access gateways)

Το παρακάτω σχήμα απεικονίζει μια χαρακτηριστική εικόνα του συστήματος που περιλαμβάνει την αποθήκη, το μητρώο συσκευών, τρεις κινητές συσκευές, έναν προσωπικό υπολογιστή με σύνδεση στο διαδίκτυο και ένα σημείο πρόσβασης δικτύου (network access point).



Σχήμα 1.1: Αρχιτεκτονική OmniStore

Ο δαίμονας της συσκευής (device daemon) διαχειρίζεται το μέσο αποθήκευσης των κινητών συσκευών. Επιβλέπει κάθε δραστηριότητα σχετική με αποθήκευση δεδομένων, ενώ παράλληλα παρακολουθεί το περιβάλλον της συσκευής για τυχόν παρουσία άλλων συσκευών. Επικοινωνεί με συσκευές που εντοπίζονται στο προσωπικό δίκτυο συσκευών του χρήστη εκτελώντας συλλογικές εργασίες διαχείρισης του χώρου αποθήκευσης. Επιπλέον επικοινωνεί περιοδικά με την αποθήκη δεδομένων (data repository) για εκτέλεση εργασιών συγχρονισμού.

Οι εφαρμογές με χρήση της βιλιοθήκης συσκευής (device library) αποκτούν πρόσβαση στο μέσο αποθήκευσης. Επιπρόσθετα, μέσω της βιλβλιοθήκης συσκευής μπορούν να αλληλεπιδράσουν με την αποθήκη δεδομένων και το μητρώο συσκευών (device registry).

Η σταθερή αποθήκη δεδομένων υλοποιείται από το δαίμονα της αποθήκης (repository daemon). Ο δαίμονας της αποθήκης αλληλεπιδρά με τους δαίμονες των συσκευών προκειμένου να συγχρονίσει τα δεδομένα κάθε συσκευής με αυτά της αποθήκης. Παρέχει πρόσβαση στα αποθηκευμένα αρχεία, τα οποία μπορούν να εντοπιστούν με σημασιολογικές ερωτήσεις αναζήτησης. Τέλος προσφέρει την υπηρεσία

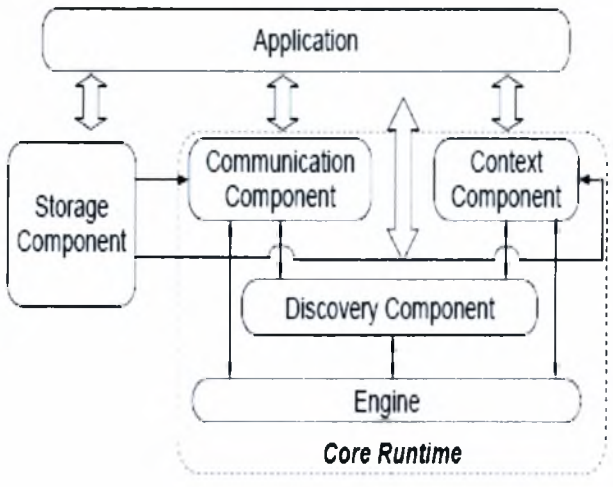
"push-caching", μέσω της οπόιας προγραμματίζονται μεταφορές αρχείων από την αποθήκη στις κινητές συσκευές. Προκειμένου να χρησιμοποιήσουν τις παραπάνω υπηρεσίες, εφαρμογές σε υπολογιστές με σύνδεση στο διαδίκτυο κάνουν χρήση της βιβλιοθήκης πελάτη αποθήκης (repository client library), ενώ εφαρμογές σε κινητές συσκευές χρησιμοποιούν την βιβλιοθήκη συσκευής.

Το μητρώο συσκευών είναι μια υπηρεσία υποδομής, η οποία καταγράφει τις συσκευές που ανήκουν στο χρήστη. Διατηρεί πληροφορίες σχετικά με τις δυνατότητές τους (πχ. υπηρεσίες που παρέχουν) καθώς και παραμέτρους διαμόρφωσης. Ο δαίμονας μητρώου (registry daemon) υλοποιεί τις προαναφερθείσες λειτουργίες και μπορεί να κληθεί είτε απο τη βιβλιοθήκη πελάτη μητρώου (registry client library), είτε απο τη βιβλιοθήκη συσκευής, για εφαρμογές σε υπολογιστές με σύνδεση στο διαδίκτυο και εφαρμογές σε κινητές συσκευές αντίστοιχα.

Η επικοινωνία των κινητών συσκευών με τις υπηρεσίες υποδομής γίνεται μέσω ειδικών συσκευών που διαθέτουν ασύρματους προσαρμογείς δικτύου και συνδέσεις στο διαδίκτυο. Οι συσκευές αυτές ονομάζονται πύλες πρόσβασης διαδικτύου και επιτρέπουν σε συσκευές του προσωπικού δικτύου συσκευών να συνδέονται στο διαδίκτυο.

1.3 Κινητές συσκευές

Οι κινητές συσκευές διαθέτουν σημαντική υπολογιστική ικανότητα και ικανότητα δικτύωσης. Το σύστημα εκτέλεσης (runtime) των συσκευών υποστηρίζει εκτέλεση εφαρμογών σε δίκτυα κινητών συσκευών χωρίς υποδομή (ad-hoc networks). Συγκεκριμένα το σύστημα εκτέλεσης παρέχει δυνατότητα επικοινωνίας, ανακάλυψης υπηρεσιών (service discovery) και ανακάλυψης πληροφοριών από το γειτονικό περιβάλλον (context information). Τα βασικά τμήματα του συστήματος εκτέλεσης παρουσιάζονται στο παρακάτω σχήμα



Σχήμα 1.2: Σύστημα εκτέλεσης (runtime)

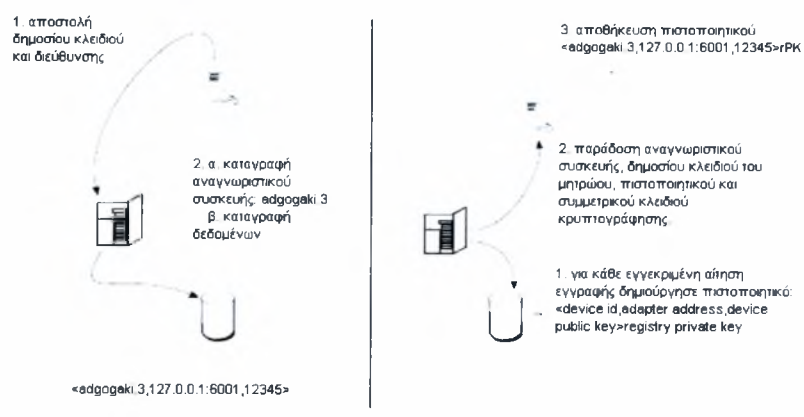
1.4 Εγγραφή συσκευών στο μητρώο

Το μητρώο συσκευών διατηρεί πληροφορία για τις συσκευές που ανήκουν στο χρήστη και παρέχει μια υπηρεσία εγγραφής συσκευών σε αυτό. Επιπρόσθετα, λειτουργεί σαν αρχή έκδοσης ψηφιακών πιστοποιητικών, η οποία εκδίδει ψηφιακά πιστοποιητικά κατά τη διάρκεια της εγγραφής μιας καινούριας συσκευής στο μητρώο. Οι συσκευές κάνοντας χρήση των πιστοποιητικών έχουν τη δυνατότητα να καθορίσουν αν ανήκουν στον ίδιο χρήστη εδραιώνοντας εμπιστοσύνη μεταξύ τους. Το μητρώο αναγνωρίζεται απο την IP διεύθυνσή του. Αναθέτει αναγνωριστικά στις συσκευές κατά τη διάρκεια της εγγραφής, τα οποία είναι μοναδικά τόσο στο περιβάλλον του μητρώου όσο και στο περιβάλλον μητρώων άλλων χρηστών. Γενομένης της εγγραφής, το μητρώο λειτουργεί σαν υπηρεσία ονομάτων για τις κινητές συσκευές του χρήστη δίνοντας τη δυνατότητα σε εφαρμογές να αναφέρονται σε αυτές με μη διφορούμενο τρόπο. Τέλος παρέχει υπηρεσίες που επιτρέπουν στις εφαρμογές να καταγράψουν ή να εξετάσουν πληροφορίες που αφορούν τις συσκευές του χρήστη και τις δυνατότητές τους. Παραδείγματος χάρη μια εφαρμογή μπορεί καταγράψει στο μητρώο ότι υποστηρίζει "διαχείριση μέσου αποθήκευσης OmniStore", ενώ μια άλλη εφαρμογή να κάνει αίτηση για λίστα συσκευών που υποστηρίζουν "διαχείριση μέσου αποθήκευσης OmniStore".

Ο δαίμονας μητρώου φιλοξενείται στη συσκευή εξυπηρετητή, η οποία είναι τοποθετημένη στην κατοικία του χρήστη. Ο χρήστης αναμένεται να ενεργοποιήσει κάθε

καινούρια συσκευή στο χώρο που είναι τοποθετημένος ο εξυπηρετητής ενεργοποιώντας τη διαδικασία εγγραφής.

Ο δαίμονας μητρώου διαφημίζει μια υπηρεσία εγγραφής στις γειτονικές συσκευές. Κατά την ενεργοποίηση μιας συσκευής γίνεται έλεγχος αν αυτή είναι εγγεγραμμένη στο μητρώο ή όχι. Οι εγγεγραμμένες συσκευές φορτώνουν το δαίμονα συσκευής και τις τοπικές εφαρμογές συνεχίζοντας την κανονική λειτουργία τους. Μη εγγεγραμμένες συσκευές μπαίνουν στην ειδική κατάσταση εγγραφής. Χρησιμοποιούν το μηχανισμό ανακάλυψης υπηρεσίων του συστήματος εκτέλεσης, αναζητώντας μια υπηρεσία εγγραφής. Κατά τη διάρκεια του πρώτου σταδίου εγγραφής, η συσκευή εντοπίζει το μητρώο και στέλνει αίτηση εγγραφής αποστέλλοντας τη διεύθυνσή της και το δημόσιο κλειδί της. Το μητρώο καταγράφει την αίτηση και αναθέτει στην συσκευή ένα μοναδικό αναγνωριστικό, το οποίο αποτελείται από το όνομα του ιδιοκτήτη της συσκευής και έναν αριθμό (εξασφαλίζεται έτσι η μοναδικότητα του αναγνωριστικού όχι μόνο στο τοπικό μητρώο αλλά και σε μητρώα άλλων χρηστών). Στη συνέχεια απαιτείται έγκριση της αίτησης από το χρήστη μέσω διαδικτυακής εφαρμογής. Μόλις ο χρήστης εγκρίνει την αίτηση περνάμε στο δεύτερο στάδιο εγγραφής. Το μητρώο αναζητά τη συσκευή προκειμένου να επικοινωνήσει μαζί της ολοκληρώνοντας τη διαδικασία εγγραφής. Όταν η συσκευή ανακαλυφθεί, το μητρώο παράγει ένα ψηφιακό πιστοποιητικό που περιλαμβάνει το αναγνωριστικό της συσκευής και το δημόσιο κλειδί της. Το πιστοποιητικό είναι ψηφιακά υπογεγραμμένο με το ιδιωτικό κλειδί του μητρώου. Στη συσκευή αποστέλλονται το αναγνωριστικό της, το ψηφιακό πιστοποιητικό, το δημόσιο κλειδί του μητρώου και ένα συμμετρικό κλειδί κρυπτογράφησης. Εγγεγραμμένες συσκευές μπορούν να χρησιμοποιήσουν το δημόσιο κλειδί του μητρώου για να επαληθεύσουν τη γνησιότητα πιστοποιητικών άλλων συσκευών. Η διαδικασία περιγράφεται στο παρακάτω σχήμα.



Σχήμα 1.3: Στάδια εγγραφής συσκευής

1.5 Λειτουργικότητες OmniStore

Το Omnistore παρέχει λειτουργικότητες βασισμένες στην υποδομή και στο προσωπικό δίκτυο συσκευών του χρήστη. Οι κυριότερες από αυτές περιγράφονται παρακάτω.

1.5.1 Λειτουργικότητες υποδομής

Η αποθήκη διαχειρίζεται το αξιόπιστο μέσο αποθήκευσης του χρήστη και παρέχει πρόσβαση σε αυτό. Σε αυτήν συλλέγονται όλα τα δεδομένα που παράγονται από τις συσκευές του χρήστη. Επιπλέον, επιτρέπει σε εφαρμογές να υποβάλλουν αιτήσεις αποστολής αρχείων από την αποθήκη σε συγκεκριμμένες συσκευές. Τέλος υποστηρίζει σημασιολογική αναζήτηση αρχείων με βάση επισημειώσεις (annotations) που προσαρτώνται στα αρχεία κατά τη δημιουργία τους. Οι επισημειώσεις είναι πληροφορίες της μορφής κλειδί-τιμή που σχετίζονται με τα αρχεία. Ακολουθεί μια αναλυτική περιγραφή των υπηρεσιών που προσφέρει η αποθήκη.

1.5.1.1 Διαδικασία συγχρονισμού (synchronization process)

Τα δεδομένα κάθε συσκευής συγχρονίζονται περιοδικά με την αποθήκη, με τη βοήθεια πυλών διαδικτύου. Όταν μια πύλη είναι διαθέσιμη λαμβάνουν χώρα τα παρακάτω γεγονότα: Δημιουργείται μια ουρά προσκομίσεως στην οποία τοποθετουνται τα αναγνωριστικά των αρχείων για τα οποία έχουν υποβληθεί push-cache αιτήσεις με προορισμό τη δεδομένη συσκευή. Στη συνέχεια δημιουργούνται αντίγραφα ασφαλείας στην αποθήκη για όλα τα αρχεία που έχουν παραχθεί/τροποποιηθεί μεταξύ δύο διαδοχικών στιγμών συγχρονισμού. Τέλος, ανακτώνται τα αρχεία απο την ουρά προσκομίσεως και αποθηκεύονται τοπικά.

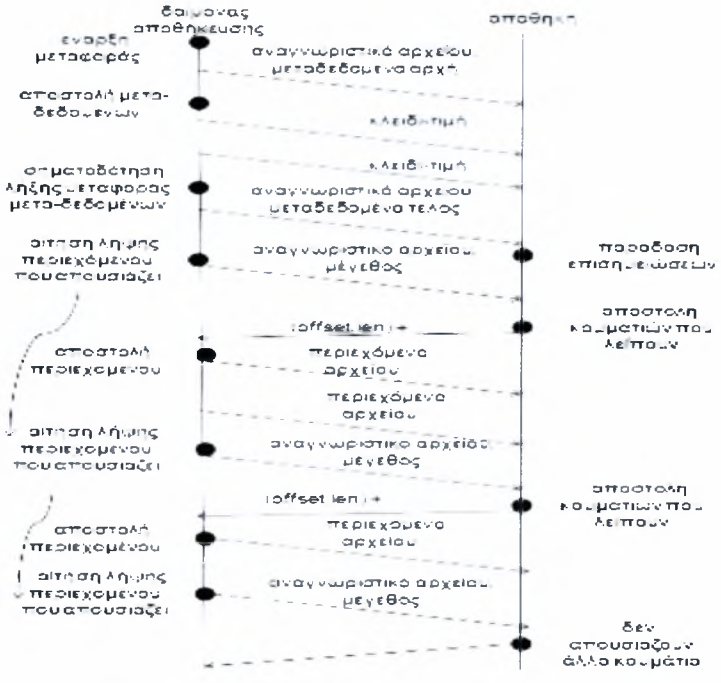
1.5.1.2 Αυτοματοποιημένη αρχειοθέτηση (automated archival)

Το Omnistore υιοθετεί την προσέγγιση "deep archival" όσον αφορά την αποθήκευση των αρχείων. Αυτή η προσέγγιση συνεπάγεται την αποθήκευση όλων των αρχείων που παράγονται από το χρήστη, χωρίς να διαγράφονται ποτέ. Η παραπάνω ιδιότητα επιτυγχάνεται μεταφέροντας στην αποθήκη όλα τα αρχεία που δημιουργούνται στις κινητές συσκευές.

Ο δαίμονας της συσκευής διατηρεί μια ουρά αντιγράφων ασφαλείας (backup queue) με τα αρχεία που δεν έχουν μεταφερθεί στην αποθήκη. Κάθε καινούριο αρχείο και κάθε αρχείο που ανοίχθηκε σε κατάσταση ανάγνωσης/εγγραφής και τροποποιήθηκε, τοποθετείται στην ουρά.

Όταν δημιουργείται ένα αρχείο προσαρτάται σε αυτό μια ειδική επισημείωση συστήματος (system annotation) με κλειδί *dirty* και τιμή αληθές. Όταν ένα αρχείο σταλεί στην αποθήκη, η τιμή της επισημείωσης γίνεται ψευδές προκειμένου να αποφευχθεί η επανατοποθέτηση του αρχείου στην ουρά. Η επισημείωση *dirty* διατηρείται ακόμα και όταν οι συσκευές είναι εκτός λειτουργίας. Κατά τη διάρκεια της ενεργοποίησης των συσκευών ελέγχεται η τιμή της επισημείωσης και η ουρά ανακατασκευάζεται ανάλογα.

Ο δαίμονας αποθήκευσης προσπαθεί περιοδικά να επικοινωνήσει με την αποθήκη. Όταν υπάρχει διαθέσιμη σύνδεση, οι εγγραφές της ουράς επεξεργάζονται με τον εξής τρόπο: Αρχικά η συσκευή στέλνει στην αποθήκη τις επισημειώσεις που είναι προσαρτημένες στο αρχείο. Η αποθήκη καταγράφει την ύπαρξη του αρχείου, τις επισημειώσεις, το μέγεθός του και το γεγονός ότι το περιεχόμενό του απουσιάζει. Η αποθήκη στέλνει λίστα με τα τμήματα του αρχείου που λείπουν. Η συσκευή στέλνει τα κομμάτια του αρχείου που ζητήθηκαν και ζητάει επαναλαμβανόμενα να στείλει και άλλα τμήματα. Όταν η αποθήκη ενημερώσει ότι δεν λείπουν άλλα τμήματα η επισημείωση *dirty* παίρνει την τιμή ψευδές και το αρχείο σβήνεται από την ουρά. Υπάρχει εγγύηση ότι άλλες συσκευές που έχουν αντίγραφο του αρχείου θα ενημερωθούν ότι αυτό αρχειοθετήθηκε, όταν επικοινωνήσουν με την αποθήκη. Η διαδικασία φαίνεται στο παρακάτω σχήμα.



Σχήμα 1.4: Πρωτόκολλο δημιουργίας αντιγράφων ασφαλείας OmniStore

1.5.1.3 Push-caching

Η αποθήκη παρέχει μια υπηρεσία αποστολής αρχείων στις κινητές συσκευές, η οποία ονομάζεται *push-caching*. Οι πελάτες μπορούν να συνδέονται στην αποθήκη και να υποβάλλουν αιτήσεις *push-caching* δηλώνοτας το αναγνωριστικό του επιθυμητού αρχείου και της συσκευής προορισμού.

Όταν ο δαίμονας της συσκευής επικοινωνεί με την αποθήκη ενημερώνεται για τυχόν *push-cache* μεταφορές αρχείων που εκκρεμούν, τις οποίες προσθέτει στην ουρά προσκόμισης (fetch-queue). Η επεξεργασία της ουράς προσκόμισης είναι παρόμοια με αυτή της ουράς δημιουργίας αντιγράφων και οδηγεί στην λήψη των αντίστοιχων αρχείων από την αποθήκη. Το πρωτόκολλο μεταφοράς αρχείων είναι ανάλογο του πρωτοκόλλου δημιουργίας αντιγράφων και ανέχεται διακοπτόμενη επικοινωνία.

Οι αιτήσεις *push-caching* μπορούν να γίνουν προαιρετικά με χρονοδιάγραμμα: μια αρχική και μια τελική χρονική στιγμή μεταξύ των οποίων το αρχείο πρέπει να βρίσκε-

ται στην συσκευή προορισμού. Επιπρόσθετα οι αιτήσεις *push-caching* μπορούν να γίνουν προαιρετικά με την επιλογή *ζωντανή-ενημέρωση* (live-update) η οποία δίνει εντολή στην αποθήκη να στείλει την τελευταία έκδοση του αρχείου στη συσκευή.

Push-cache αιτήσεις υποβάλλονται στην αποθήκη μέσω της βιλβλιοθήκης αποθήκης. Αξίζει να σημειωθεί ότι δεν είναι απαραίτητο να είναι προσβάσιμη η συσκευή προορισμού τη στιγμή που υποβάλλονται τέτοιες αιτήσεις στην αποθήκη. Δίνεται συνεπώς η δυνατότητα στους χρήστες/εφαρμογές να προγραμματίσουν μεταφορές αρχείων σε συσκευές, χωρίς να είναι απαραίτητη η παρουσία τόσο του αρχείου όσο και της συσκευής προορισμού τη στιγμή δημιουργίας της αίτησης.

1.5.1.4 Υπηρεσίες εφαρμογών (application services)

Οι εφαρμογές μπορούν να χρησιμοποιήσουν τις υπηρεσίες που παρέχει η αποθήκη χρησιμοποιώντας την αντίστοιχη βιβλιοθήκη αποθήκης. Συγκεκριμένα με χρήση της μεθόδου lookupFiles() επιστρέφονται τα αρχεία των οποίων οι επισημειώσεις ταυτίζονται με τις επισημειώσεις που περνώνται στην μέθοδο σαν όρισμα. Οι ερωτήσεις μπορούν να γίνουν τόσο με βάση το κλειδί της επισημείωσης (key) όσο και την τιμή της (value). Αιτήσεις push-cahe μπορούν να προγραμματιστούν με κλήση της μεθόδου submitPCR(), η οποία παίρνει σαν όρισμα το αναγνωριστικό του αρχείου, το αναγνωριστικό της συσκευής, τη χρονική περίοδο που πρέπει να γίνει η μεταφορά και τέλος αν η συσκευή πρέπει να ενημερώνεται με μελλοντικές εκδόσεις του αρχείου.

1.5.2 Λειτουργικότητες προσωπικού δικτύου συσκευών

Δεδομένης της ικανότητας των κινητών συσκευών να επικοινωνούν μεταξύ τους (ad-hoc networking), οι συσκευές συνεργάζονται παρέχοντας επιπλέον λειτουργικότητες στο χρήστη. Οι κυριότερες λειτουργίες που προσφέρει το Omnistore που βασίζονται στην ικανότητα επικοινωνίας των κινητών συσκευών είναι:

- Αυτοματοποιημένη δημιουργία επισημειώσεων με σημασιολογικές πληροφορίες απο πολλαπλές πηγές.

- Μεταφορά αρχείων από μια συσκευή στην άλλη για αύξηση της διαθεσιμότητας και κατανομή του φόρτου αποθηκέυσης.

- Υποστήριξη απομακρυσμένης πρόσβασης αρχείων που επιτρέπει στις εφαρμογές να εκτελούν λειτουργίες Εισόδου/Εξόδου (E/E) σε αρχεία που βρίσκονται σε οποιαδήποτε συσκευή του προσωπικού δικτύου.

1.5.2.1 Δημιουργία επισημειώσεων με βάση το γειτονικό περιβάλλον (context-based annotation)

Το Omnistore δημιουργεί αυτόματα επισημειώσεις χρησιμοποιώντας την ικανότητα αίσθησης του περιβάλλοντος που έχουν οι συσκευές του προσωπικού δικτύου. Οι επισημειώσεις δημιουργούνται απο πλειάδες που διατηρούνται απο ειδικό τμήμα του συστήματος εκτέλεσης των συσκευών (runtime's context component). Στόχος είναι να καταγραφεί η κατάσταση του περιβάλλοντος τη στιγμή που δημιουργείται ένα αρχείο. Η διαδικασία δημιουργίας επισημειώσεων είναι η εξής: όταν δημιουργείται το αρχείο η βιβλιοθήκη συσκευής λαμβάνει το σύνολο των πλειάδων από το στοιχείο περιβάλλοντος του συστήματος εκτέλεσης. Τα ζευγάρια κλειδί/τιμή των πλειάδων χρησιμοποιούνται για να κατασκευαστεί η λίστα επισημειώσεων.

1.5.2.2 Δημιουργία αντιγράφων και εξοικονόμιση χώρου στις συσκευές (replication and off-loading)

Το Omnistore δημιουργεί ελεύθερο χώρο στις συσκευές που το μέσο αποθήκευσής τους γεμίζει. Επιπρόσθετα, δημιουργούνται αντίγραφα σημαντικών αρχείων για αυξημένη διαθεσιμότητα. Όσον αφορά τη δημιουργία ελεύθερου χώρου, χρησιμοποιούνται δύο παράμετροι διαμόρφωσης που δείχνουν τον ελάχιστο επιτρεπτό ελεύθερο χώρο και τον επιθυμητό ελεύθερο χώρο. Μόλις ο ελεύθερος χώρος πέσει κάτω από τον ελάχιστο επιτρεπτό ενεργοποιείται η διαδικασία συγκομιδής απορριμμάτων. Υποψήφια προς διαγραφή αρχεία είναι αυτά για τα οποία έχει δημιουργηθεί αντίγραφο ασφαλείας στην αποθήκη και αυτά που δεν αναμένεται να βρίσκονται στην συσκευή στο άμεσο μέλλον. Η πρώτη συνθήκη ελέγχεται επιθεωρώντας την επισημείωση *dirty*, ενώ η δεύτερη επιθεωρώντας τις επισημειώσεις *avail-start* και *avail-end*. Αρχεία σβήνονται μέχρι να εξασφαλιστεί ο επιθυμητός ελεύθερος χώρος. Είναι πιθανό, πριν την εξασφάλιση του επιθυμητού ελεύθερου χώρου να μην υπάρχουν άλλα αρχεία που πληρούν τις συνθήκες διαγραφής. Τότε η συσκευή διαγράφει το αρχείο αφού πρώτα δημιουργήσει αντίγραφο σε κάποια γειτονική συσκευή, η οποία πλέον επωμίζεται την ευθύνη δημιουργίας αντιγράφου ασφαλείας στην αποθήκη. Το πρωτόκολλο μεταφοράς αρχείων σε γειτονικές συσκευές είναι ανάλογο του πρωτοκόλλου δημιουργίας αντιγράφων ασφαλείας στην αποθήκη και επιτρέπει διακοπτόμενη επικοινωνία.

Μια ακόμη δραστηριότητα που λαμβάνει χώρα μεταξύ των κινητών συσκευών είναι η αντιγραφή σημαντικών αρχείων. Για να ενεργοποιηθεί η παραπάνω διαδικασία χρησιμοποιείται η επισημείωση με κλειδί *replicate-count* η οποία λαμβάνει τιμή έναν ακέραιο που υποδεικνύει το πλήθος των αντιγράφων που πρέπει να δημιουργηθούν. Το πρωτόκολλο δημιουργίας αντιγράφων είναι ανάλογο του πρωτοκόλλου μεταφοράς αρχείων στις γειτονικές συσκευές.

1.5.2.3 Κατανεμημένη αναζήτηση και πρόσβαση αρχείων (distributed lookup and access)

Η αναζήτηση αρχείων σε σημασιολογικά συστήματα αρχείων δεν περιορίζεται στη χρήση ονομάτων αρχείων, αλλά μπορεί να χρησιμοποιηθεί οποιαδήποτε επισημείωση. Η βιβλιοθήκη της συσκευής επιτρέπει στις εφαρμογές να δημιουργήσουν *εργασίες αναζήτησης επισημειώσεων*, οι οποίες εγγράφονται στο δαίμονα της συσκευής. Στα αποτελέσματα των εργασιών αναζήτησης συγκαταλλέγονται τοπικά αλλά και απομακρυσμένα αρχεία από γειτονικές συσκευές. Οι δαίμονες των συσκευών ενημερώνονται για την άφιξη/αναχώρηση συσκευών με ικανότητα αποθήκευσης από τον πυρήνα του συστήματος εκτέλεσης (core runtime). Νεοαφιχθείσες συσκευές ερωτώνται για αρχεία που ταιριάζουν με τους όρους αναζήτησης που ορίζονται στις εργασίες αναζήτησης. Η απομάκρυνση συσκευών από το προσωπικό δίκτυο συσκευών οδηγεί στην απομάκρυνση των αρχείων της συσκευής από τη λίστα με τα αρχεία που ταιριάζουν με τα κριτήρια αναζήτησης.

Οι λειτουργίες πρόσβασης αρχείων είναι παρόμοιες με αυτές των τυπικών συστημάτων αρχείων. Εξαίρεση αποτελεί το γεγονός ότι απαιτείται τοπικότητα του αρχείου προκειμένου αυτό να τροποποιηθεί. Άνοιγμα ενός αρχείου σε κατάσταση ανάγνωσης/εγγραφής οδηγεί στην δημιουργία αντιγράφου τοπικά στην συσκευή. Το άνοιγμα αρχείου μόνο για ανάγνωση γίνεται απ ′ ευθείας στην απομακρυσμένη συσκευή.

Κεφάλαιο 2

Ασφαλής συνεργασία σε δίκτυα κινητών συσκευών

2.1 Εισαγωγή

Ένα ασφαλές δίκτυο πρέπει να έχει τα παρακάτω πέντε χαρακτηριστικά [7] : αυθεντικοποίηση, μη-απάρνηση, εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Αυθεντικοποίηση είναι η εξακρίβωση της ταυτότητας του χρήστη προτού του χορηγηθεί άδεια πρόσβασης στο δίκτυο. Μη-απάρνηση είναι η διαδικασία επαλήθευσης ότι τα δεδομένα στάλθηκαν με τα διαπιστευτήρια κάποιου χρήστη με τέτοιο τρόπο ώστε να να είναι αδύνατη η απάρνηση της συσχέτισης των δεδομένων με την ταυτότητα του χρήστη. Εμπιστευτικότητα είναι διαβεβαίωση ότι τα δεδομένα αποκαλύπτονται μόνο σε εξουσιοδοτημένα άτομα. Η εμπιστευτικότητα συνήθως επιτυγχάνεται με χρήση κρυπτογραφικών τεχνικών. Η ακεραιότητα δεδομένων είναι η διαβεβαίωση ότι τα δεδομένα δεν τροποποιήθηκαν κατά τη διάρκεια της μεταφοράς. Διαφέρει από την εμπιστευτικότητα με την έννοια ότι επιτρέπει ανίχνευση αλλαγών στα δεδομένα. Τέλος το πέμπτο χαρακτηριστικό, η διαθεσιμότητα είναι το ποσοστό του χρόνου στο οποίο το σύστημα είναι διαθέσιμο. Στην προσέγγισή μας για εισαγωγή ασφάλειας στο σύστημα Omnistore θεωρούμε την αυθεντικοποίηση τον πρώτο μηχανισμό ασφάλειας και άμυνας εναντίον κακόβουλης δικτυακής δραστηριότητας, διότι δεν είναι δυνατή η εδραίωση ενός ασφαλούς καναλιού επικοινωνίας, αν δεν γίνεται αμοιβαία αυθεντικοποίηση των οντοτήτων που συμμετέχουν στην επικοινωνία.

2.2 Απαιτήσεις αυθεντικοποίησης σε δίκτυα κινητών συσκευών

Τα δίκτυα κινητών συσκευών έχουν ειδικές απαιτήσεις όσον αφορά την αυθεντικοποίηση των κόμβων/συσκευών. Οι κυριότερες απαιτήσεις ειναι [5] :

- **Ισχυρή αυθεντικοποίηση:** ορίζεται η διαδικασία επικύρωσης της ταυτότητας μιας οντότητας με χρήση αποθηκευμένων διαπιστευτηρίων, τα οποία παράγονται με κρυπτογραφικές μεθόδους. Τα συστήματα κινητής υπολογιστικής είναι ευαίσθητα σε επιθέσεις υποκλοπής, μέσω παθητικής παρακολούθησης (eavesdropping) συνεπώς τα διαπιστευτήρια, καθώς και τα κρυπτογραφικά κλειδιά των συσκευών πρέπει να παραδίδονται σε αυτές με ασφαλή τρόπο.

- **Ευκολία στη χρήση:** στα συστήματα κινητής υπολογιστικής ο χρήστης είναι εν κινήσει και συνεπώς πρέπει να ελαχιστοποιηθεί η αλληλεπίδρασή του με τη συσκευή προκειμένου να γίνει αυθεντικοποίηση αυτής στο δίκτυο. Π.χ πρέπει να αποφεύγεται η χρήση κωδικών προκειμένου να αποκτήσει η συσκευή πρόσβαση στο δίκτυο.

- **Κλιμάκωση:** τα δίκτυα κινητής υπολογιστικής ποκίλουν ως προς το μέγεθος και μπορούν να αποτελούνται από λίγους μέχρι αρκετές δεκάδες κόμβους. Όσο το μέγεθος του δικτύου μεγαλώνει η αυθεντικοποίηση γίνεται πιο πολύπλοκη. Το κόστος της διαδικασίας αυθεντικοποίσης (αριθμός κρυπτογραφικών λειτουργιών, αριθμός μηνυμάτων) αυξάνεται ραγδαία καθώς προστίθενται νέοι κόμβοι στο δίκτυο. Ένα πρωτόκολλο αυθεντικοποίησης πρέπει να έχει ικανότητα κλιμάκωσης και να μπορεί να χειρίζεται μια ικανοποιητική αύξηση του αριθμού των κόμβων του δικτύου.

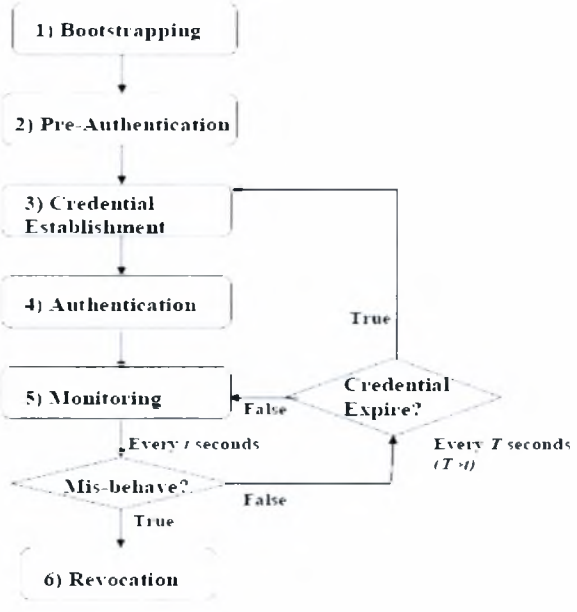
- **Μικρός φόρτος:** εξαιτίας του περιορισμένου εύρους ζώνης, της περιορισμένης υπολογιστικής ισχύος και της απαίτησης χαμηλής κατανάλωσης ενέργειας, το πρωτόκολλο αυθεντικοποίησης πρέπει να εισάγει όσο το δυνατόν λιγότερο φόρτο στο δίκτυο.

- **Υποστήριξη ανάκλησης:** πρέπει να υπάρχει δυνατότητα ανάκλησης των διαπιστευτηρίων των συσκευών και απομάκρυνσή τους από το δίκτυο, π.χ σε περίπτωση που κάποια συσκευή κλαπεί.

- **Διαλειτουργικότητα:** υπάρχει απαίτηση το σχήμα αυθεντικοποίησης ενός δικτύου να μπορεί να συνεργαστεί με το σχήμα αυθεντικοποίησης ενός άλλου δικτύου με αποτέλεσμα τα δύο δίκτυα να μπορούν εύκολα να ενωθούν.

2.3 Στοιχεία ισχυρής διαδικασίας αυθεντικοποίησης

Μια λύση του προβλήματος ισχυρής αυθεντικοποίησης περιλαμβάνει τα παρακάτω έξι βήματα: boot-strapping, προ-αυθεντικοποίηση (*pre-authentication*), εδραίωση διαπιστευτηρίων (*credential establishment*), αυθεντικοποίηση (*authentication*), παρακολούθηση (*monitoring*) και ανάκληση (*revocation*). [2]



Σχήμα 2.1: Στοιχεία ισχυρής αυθεντικοποίησης

Ακολουθεί περιγραφή των παραπάνω βημάτων:

- **Bootstrapping** είναι το βήμα στο οποίο μια οντότητα λαμβάνει/δημιουργεί ένα διαπιστευτήριο. Το διαπιστευτήριο μπορεί να είναι κάτι που διαθέτει η οντότητα (π.χ κλειδί), κάτι που γνωρίζει (π.χ συνθηματικό) ή κάτι που είναι (π.χ βιομετρικό χαρακτηριστικό). Π.χ μπορεί να εφαρμοστεί bootstrapping αναθέτοντας ένα αρχικό κλειδί σε κάθε κόμβο που εισέρχεται στο δίκτυο.

- **Προ-αυθεντικοποίηση** είναι το βήμα στο οποίο η οντότητα παρουσιάζει τα διαπιστευτήρια προκειμένου να αποδείξει ότι έχει δικαίωμα πρόσβασης σε προστατευμένες πληροφορίες/υπηρεσίες. Εναλλακτικά προ-αυθεντικοποίηση ορίζεται η αρχική ανταλλαγή διαπιστευτηρίων.

- **Δημιουργία διαπιστευτηρίων:** Σε αυτό το βήμα δημιουργούνται καινούρια διαπιστευτήρια τα οποία η οντότητα θα χρησιμοποιήσει σαν απόδειξη της ταυτότητας της. Διαπιστευτήριο μπορεί να αποτελέσει ένα συμμετρικό κλειδί

κρυπτογράφησης, ένα ζεύγος δημόσιου/ιδιωτικού κλειδιού, ένα ψηφιακό πιστοποιητικό. Η δημιουργία των διαπιστευτηρίων πρέπει να συνδέεται με μια ημερομηνία λήξης ώστε να είναι απαραίτητη η ανανέωσή τους.

- **Αυθεντικοποίηση:** Σε αυτό το βήμα γίνεται επαλήθευση των ταυτοτήτων των οντοτήτων που συμμετέχουν στην επικοινωνία, με βάση τα διαπιστευτήρια τους.

- **Έλεγχος:** Παρακολουθείται η συμπεριφορά μιας αυθεντικοποιημένης οντότητας. Μια οντότητα η οποία τίθεται σε κίνδυνο (π.χ κλοπή) ή ''παρεκτρέπεται'' παύει να έχει δικαίωμα χρήσης πόρων/υπηρεσιών και τα διαπιστευτήρια της ανακαλούνται. Η συχνότητα ελέγχου και τα κριτήρια κακής συμπεριφοράς καθορίζονται από τις εφαρμογές.

- **Ανάκληση:** Αυτό το βήμα ασχολείται με δύο ζητήματα: 1) πότε πρέπει μια οντότητα να μπει στη λίστα ανάκλησης, 2) πώς θα ενημερωθούν οι υπόλοιπες οντότητες σχετικά με την ανάκληση.

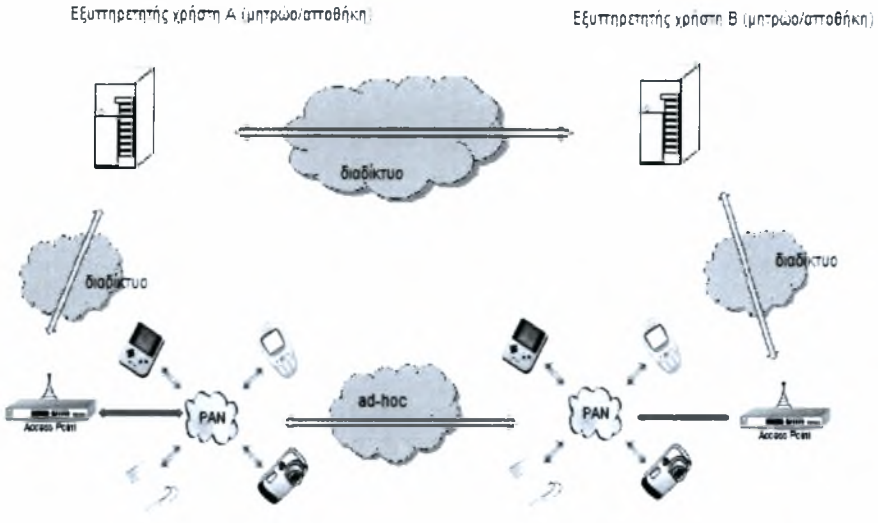
Στο επόμενο κεφάλαιο θα προτείνουμε μια λύση στο πρόβλημα ασφαλούς συνεργασίας προσωπικών συσκευών (κινητών) διαφορετικών χρηστών, βασιζόμενοι στο σύστημα Omnistore. Θα ασχοληθούμε κυρίως με το πρόβλημα της αυθεντικοποίησης προτείνοντας ένα σύστημα που πληρεί τις έξι απαιτήσεις και περιλαμβάνει τα έξι στοιχεία ισχυρής αυθεντικοποίησης. Παρόλο που κύριο μέλημα της δουλειάς μας είναι η αυθεντικοποίηση οντοτήτων, εξασφαλίζεται και εμπιστευτικότητα δεδομένων με χρήση κρυπτογραφικών τεχνικών.

Κεφάλαιο 3

Επέκταση του συστήματος **OmniStore**

Σε αυτό το κεφάλαιο θα παρουσιάσουμε τις προσθήκες που έγιναν στο σύστημα OmniStore και πώς μέσα από αυτές δίνεται λύση στο πρόβλημα της ασφαλούς συνεργασίας μεταξύ προσωπικών συσκευών διαφορετικών χρηστών.

Σκοπός της δουλειάς μας είναι να επιτρέψουμε στις συσκευές δύο διαφορετικών χρηστών του συστήματος OmniStore να συνεργάζονται. Αρχικά περιγράφεται η διαδικασία σύναψης συνεργασίας μεταξύ δύο διαφορετικών χρηστών του συστήματος. Στη συνέχεια ακολουθεί η περιγραφή της διαδικασίας μέσω της οποίας εδραιώνεται εμπιστοσύνη μεταξύ των συσκευών. Έπειτα αναλύεται η διαδικασία αυθεντικοποίησης οντοτήτων και ο τρόπος με τον οποίο εξασφαλίζεται εμπιστευτικότητα δεδομένων. Τέλος γίνεται μια αξιόλογηση της λύσης σε σχέση με τις απαιτήσεις ισχυρής αυθεντικοποίησης που συζητήθηκαν στο προηγούμενο κεφάλαιο.



Σχήμα 3.1: Επέκταση συστήματος OmniStore

3.1 Εισαγωγή

Κάθε χρήστης διαθέτει μια συσκευή εξυπηρετητή στην οποία τρέχουν οι υπηρεσίες υποδομής (repository service, registry service). Η registry service χαρακτηρίζεται από το όνομα του χρήστη της (reg user) και την IP διεύθυνσή της. Κάθε χρήστης διαθέτει επιπλέον ένα σύνολο κινητών συσκευών. Οι συσκευές αυτές είναι εγγεγραμμένες στο μητρώο του χρήστη. Κάθε συσκευή διαθέτει ένα μοναδικό αναγνωριστικό (devId) το οποίο είναι της μορφής " όνομα χρήστη.αριθμός συσκευής ". Π.χ μια συσκευή του χρήστη με όνομα adgogaki θα μπορούσε να έχει αναγνωριστικό *adgogaki.2*. Κάθε συσκευή διαθέτει επίσης ένα ζεύγος ιδιωτικό/ δημόσιο κλειδί (SK_dev/PK_dev), ένα συμμετρικό κλειδί που μοιράζεται με το μητρώο και ένα ψηφιακό πιστοποιητικό που συνδέει το αναγνωριστικό της με το δημόσιο κλειδί της. Το πιστοποιητικό είναι υπογεγραμμένο με το ιδιωτικό κλειδί του μητρώου (SK_reg).

Σκοπός του πρωτοκόλλου σύναψης συνεργασίας είναι η ασφαλής ανταλλαγή των δημοσίων κλειδιών των μητρώων. Έτσι ο κάθε χρήστης είναι σε θέση να ελέγχει την αυθεντικότητα των πιστοποιητικών που παρουσιάζουν συσκευές που ανήκουν στο χρήστη με τον οποίο σύναψε συνεργασία.

3.2 Σύναψη συνεργασίας μεταξύ των χρηστών Α και Β

Το μητρώο του χρήστη Α (regA) διατηρεί μια λίστα με τις εκκρεμείς αιτήσεις συνεργασίας (pending collabs) με κάθε άλλο μητρώο (regB) με εγγραφές της μορφής <active/passive, regB user, regB IP address, shared key AB>. Διαθέτει επίσης μια λίστα με επικυρωμένες αιτήσεις συνεργασίας (acked collabs) με κάθε άλλο μητρώο (regB), με εγγραφές της μορφής <regB user, regB IP address, regB public key>.

Αν οι χρήστες Α και Β επιθυμούν να συνάψουν συνεργασία, τότε: Σε πρώτη φάση, Οι δύο χρήστες συμφωνούν προφορικά σε μία μυστική λέξη (passphrase), μέσω της οποίας παράγουν ένα κοινό συμμετρικό κλειδί. Επιπρόσθετα συμφωνούν στο ποιός από τους δύο θα αναλάβει το ενεργό μέρος της διαδικασίας. Θεωρούμε οτι οι δύο χρήστες γνωρίζουν τόσο τις διευθύνσεις όσο και τα ονόματα των χρηστών των μητρώων με τους οποίους επιθυμούν να συνάψουν συνεργασία. (regA/regB IP address και regA/regB user.)

Σε δεύτερη φάση μέσω κατάλληλης διαδικτυακής εφαρμογής, ο χρήστης Α δημιουργεί ενεργητική αίτηση συνεργασίας εισάγοντας το όνομα του χρήστη Β (regB user), την IP διέυθυνση του μητρώου Β (regB IP address) και τέλος την συμφωνημένη μυστική λέξη. Αντίστοιχα ο χρήστης Β δημιουργεί παθητική αίτηση συνεργασίας εισάγοντας το όνομα του χρήστη Α (regA user), την IP διέυθυνση του μητρώου Α (regA IP address) και την συμφωνημένη μυστική λέξη. Η παραπάνω διαδικασία μπορεί να γίνει ασύγχρονα.

Μετά την ολοκλήρωση της δεύτερης φάσης το μητρώο Α έχει δημιουργήσει την εγγραφή <active, regB user, regB IP address, secret key AB> και ο Β την εγγραφή <passive, regA user, regA IP address, shared key AB>. Στην συνέχεια το μητρώο Α αναλαμβάνει να επικοινωνήσει με το μητρώο Β ώστε να επικυρωθεί η συνεργασία, ακολουθώντας κατάλληλο πρωτόκολλο, που περιγράφεται στον παρακάτω ψευδοκώδικα:

Algorithm 1 regA: processing of active collaboration request with regB

```
1: while (<active, regB_user, regB_address, K_AB> in pending colabs) do
2:    send_to (regB_address, <C_REQ, regA_address, regA_user,
      [ regA_address, PK_regA] K_AB>)
3:    wait (T);
4: end while
```

Algorithm 2 regA: processing of incoming requests and acks

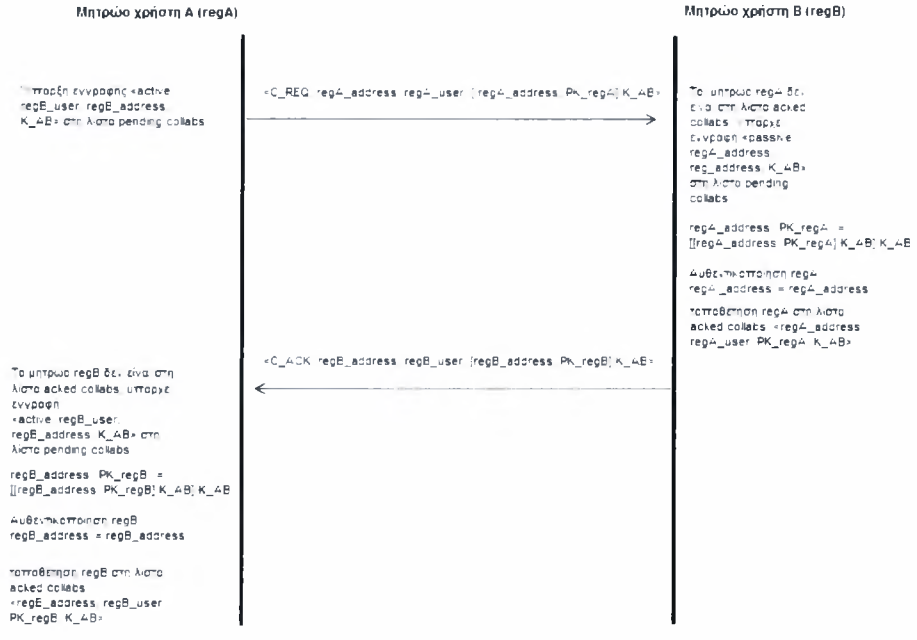
```
1: while (true) do
2:   m := get_next_msg();
3:   if (m = <C_REQ,regB_address,regB_user,[regB_address,PK_regB]K_AB>)
     then
4:     if (E <regB_address,regB_user,PK_regB,K_AB> in acked collabs) then
5:       regB_address',PK_regB' := [[regB_address, PK_regB]K_AB]K_AB
6:       if (regB_address' = regB_address) then
7:         send_to(regB_address,<C_ACK,regA_address,regA_user,
           [regA_address,PK_regA]K_AB>)
8:       end if
9:     else if (E <passive,regB_address,regB_user,K_AB> in pending collabs)
       then
10:      regB_address',PK_regB' := [[regB_address, PK_regB]K_AB]K_AB
11:      if (regB_address' = regB_address) then
12:        remove entry <passive,regB_address,regB_user,K_AB> from pen-
           ding collabs
13:        add entry <regB_address,regB_user,PK_regB,K_AB> in acked col-
           labs
14:        send_to(regB_address,<C_ACK,regA_address,regA_user,
           [regA_address,PK_regA]K_AB>)
15:      end if
16:    end if
17:  else if (m = <C_ACK,regB_address,regB_user,[regB_address,PK_regB]K_-
     AB) then
18:    if (!E <regB_address,regB_user,PK_regB,K_AB> in acked collabs) then
19:      if (E <active,regB_address,regB_user,K_AB> in pending collabs)
         then
20:        regB_address',PK_regB' := [[regB_address, PK_regB]K_AB]K_AB
21:        if (regB_address' = regB_address) then
22:          remove entry <active,regB_address,regB_user,K_AB> from pen-
             ding collabs
23:          add entry <regB_address,regB_user,PK_regB,K_AB> in acked
             collabs
24:        end if
25:      end if
26:    end if
27:  end if
28: end while
```

Το μητρώο regA ελέγχει τη λίστα με τις εκκρεμείς αιτήσεις συνεργασίας (pending collabs) με κάθε άλλο μητρώο regB. Για κάθε "active" εγγραφή που βρίσκει δημιουργεί αίτηση συνεργασίας στο αντίστοιχο μητρώο regB . Στέλνει μήνυμα αίτησης συνεργασίας που περιλαμβάνει: 1) το όνομα χρήστη του μητρώου regA (regA_user), 2) την IP διεύθυνση του μητρώου regA (regA_address), 3) την IP διεύθυνση και το δημόσιο κλείδι του μητρώου regA (PK_regA) κρυπτογραφημένα με το προσυμφωνημένο μυστικό κλειδί K_AB, στο οποίο συμφώνησαν προφορικά οι χρήστες των μητρώων regA και regB (βρίσκεται αποθηκευμένο στη λίστα pending collabs)

Στη συνέχεια το μητρώο regB λαμβάνει το μήνυμα αίτησης. Αρχικά ελέγχει μήπως υπάρχει ήδη συνεργασία με το μητρώο regA (έλεγχος της λίστας acked collabs). Σε περίτωση που υπάρχει, αποκρυπτογραφεί το κρυπτογραφημένο κομμάτι του μηνύματος με χρήση του προσυμφωνημένου μυστικού κλειδιού K_AB και ελέγχει αν η μη κρυπτογραφημένη διεύθυνση που εστάλη είναι ίδια με την κρυπτογραφημένη. Με αυτόν τον τρόπο επιτυγχάνεται αυθεντικοποίηση του μητρώου regA. Σε περίπτωση που ο έλεγχος γίνει με επιτυχία, το μητρώο regA αποστέλλει στο μητρώο regB μήνυμα επικύρωσης συνεργασίας που περιλαμβάνει: 1) το όνομα χρήστη του μητρώου regB (regB_user), 2) την IP διεύθυνση του μητρώου regB (regB_address), 3) την IP διεύθυνση και το δημόσιο κλείδι του μητρώου regB (PK_regB) κρυπτογραφημένα με το προσυμφωνημένο μυστικό κλειδί K_AB. Σε περίπτωση που δεν υπάρχει επικυρωμένη συνεργασία με το μητρώο regA, γίνεται έλεγχος της λίστας με τις εκκρεμείς αιτήσεις συνεργασίας (pending collabs) για ύπαρξη "passive" αίτησης συνεργασίας με το μητρώο regA. Αν υπάρχει παθητική αίτηση συνεργασίας τότε το μητρώο regB αποκρυπτογραφεί το κρυπτογραφημένο κομμάτι του μηνύματος με χρήση του προσυμφωνημένου μυστικού κλειδιού K_AB και ελέγχει αν η μη κρυπτογραφημένη διεύθυνση που εστάλη είναι ίδια με την κρυπτογραφημένη αυθεντικοποιώντας έτσι το μητρώο regA. Αν ο έλεγχος γίνει με επιτυχία τότε το μητρώο regB σβήνει την παθητική αίτηση συνεργασίας απο την αντίστοιχη λίστα και τοποθετεί το μητρώο regA στη λίστα με τις επικυρωμένες συνεργασίες γράφοντας 1) το όνομα χρήστη του μητρώου regA (regA_user), 2) την IP διεύθυνση του μητρώου regA (regA_address), 3) το δημόσιο κλείδι του μητρώου regA (PK_regA), 4) το προσυμφωνημένο μυστικό κλειδί K_AB. Τέλος στέλνει μήνυμα επικύρωσης συνεργασίας στο μητρώο regA που περιλαμβάνει: 1) το όνομα χρήστη του μητρώου regB (regB_user), 2) την IP διεύθυνση του μητρώου regB (regB_address), 3) την IP διεύθυνση και το δημόσιο κλείδι του μητρώου regB (PK_regB) κρυπτογραφημένα με το προσυμφωνημένο μυστικό κλειδί K_AB.

Το μητρώο regA λαμβάνει το μήνυμα επικύρωσης συνεργασίας απο το μητρώο regB. Αρχικά επιβεβαιώνει ότι δεν υπάρχει συνεργασία με το μητρώο regB ελέγχοντας τη λίστα με τις επικυρωμένες συνεργασίες. Έπειτα γίνεται έλεγχος της λίστας με τις εκκρεμείς αιτήσεις συνεργασίας (pending collabs) για ύπαρξη "active" αίτη-

σης συνεργασίας με το μητρώο regB. Σε περίπτωση που υπάρχει αίτηση συνεργασίας το μητρώο regA αποκρυπτογραφεί το κρυπτογραφημένο κομμάτι του μηνύματος με χρήση του προσυμφωνημένου μυστικού κλειδιού K_AB και ελέγχει αν η μη κρυπτογραφημένη διεύθυνση που εστάλη είναι ίδια με την κρυπτογραφημένη αυθεντικοποιώντας έτσι το μητρώο regB. Αν ο έλεγχος πραγματοποιηθεί με επιτυχία διαγράφει την ενεργητική αίτηση συνεργασίας με το μητρώο regB από τη λίστα με τις εκκρεμείς αιτήσεις συνεργασίας και τοποθετεί το μητρώο regB στη λίστα με τις επικυρωμένες συνεργασίες γράφοντας 1) το όνομα χρήστη του μητρώου regB (regB_user), 2) την IP διεύθυνση του μητρώου regB (regB_address), 3) το δημόσιο κλείδι του μητρώου regB (PK_regB), 4) το προσυμφωνημένο μυστικό κλειδί K_AB.



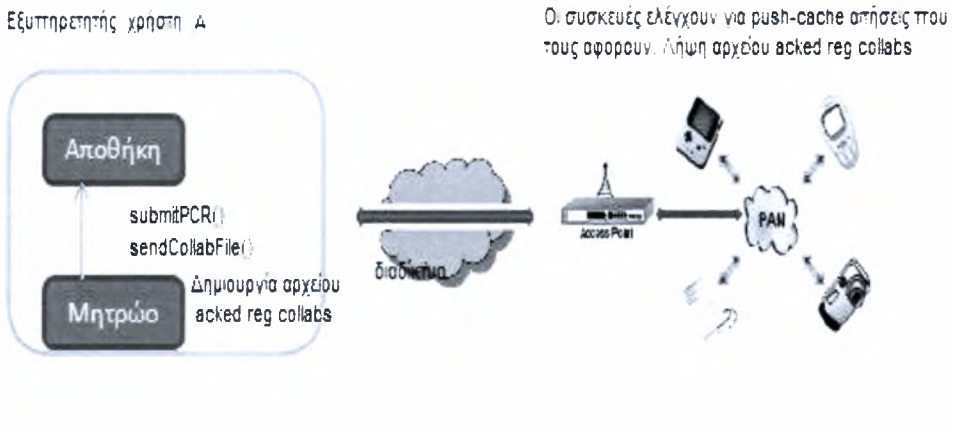
Σχήμα 3.2: Σύναψη συνεργασίας μεταξύ μητρώου regA και regB

3.2.1 Ενημέρωση συσκευών για τη σύναψη συνεργασίας

Οι κινητές συσκευές κάθε χρήστη πρέπει να ενημερώνονται κάθε φορά που συνάπτεται μια συνεργασία και να λαμβάνουν το δημόσιο κλειδί του αντίστοιχου μητρώου. Αυτό επιτυγχάνεται με χρήση της υπηρεσίας push-caching που παρέχει η αποθήκη δεδομένων. Κάθε φορά που δημιουργείται μια συνεργασία, το μητρώο δημιουργεί ένα αρχείο που περιέχει όλες τις συνεργασίες. Συγκεκριμμένα περιέχει δεδομένα της μορφής <registry address, registry user, registry's public key>. Πρέπει να σημειωθεί ότι η πρώτη εγγραφή στο αρχείο αντιστοιχεί στα χαρακτηριστικά του ίδιου

του μητρώου που δημιουργεί το αρχείο. Το αρχείο αποστέλλεται στην αποθήκη δεδομένων με χρήση της μεθόδου sendCollabFile() της βιβλιοθήκης αποθήκης. Στην συνέχεια δημιουργείται push-cache αίτηση αποστολής του αρχείου συνεργασιών με προορισμό κάθε συσκευή που ανήκει στο χρήστη. Όπως αναφέρθηκε στην περιγραφή του Omnistore οι συσκευές επικοινωνούν περιοδικά με την αποθήκη ελέγχοντας για εκκρεμείς push-cache αιτήσεις. Συνεπώς λαμβάνουν το αρχείο με τις συνεργασίες, το οποίο αποθηκεύουν τοπικά στο αρχείο (acked reg collabs).

Το αρχείο με τις συνεργασίες στην ουσία περιέχει αντιστοιχίες μητρώο-όνομα χρήστη/δημόσιο κλειδί. Αν κάποιος επέμβει σε αυτό το αρχείο αλλάζοντας το δημόσιο κλειδί, είναι σε θέση να κατασκευάζει πλαστά πιστοποιητικά συσκευών χρησιμοποιώντας το δικό του ζεύγος δημόσιο/ιδιωτικό κλειδί, τα οποία όμως αυθεντικοποιούνται με επιτυχία. Συνεπώς το αρχείο με τις συνεργασίες μεταφέρεται κρυπτογραφημένο στις συσκευές με χρήση του μυστικού κλειδιού που μοιράζεται το μητρώο με τις συσκευές.



Σχήμα 3.3: Ενημέρωση συσκευών για τη σύναψη συνεργασίας

3.3 Εμπιστοσύνη μεταξύ κινητών συσκευών

Κάθε συσκευή διατηρεί ένα αρχείο με τις συσκευές τις οποίες εμπιστεύεται (acked dev collabs) με εγγραφές<owner username, device Id, device address, device public key>. Διατηρεί επίσης ένα αρχείο για τις συσκευές με τις οποίες η ίδια έχει ξεκινήσει την διαδικασία επιβεβαίωσης συνεργασίας, με εγγραφές της μορφής <device id, random seed, timestamp>. Κάθε συσκευή εκπέμπει περιοδικά μήνυμα παρουσίας (heartbeat) με το αναγνωριστικό της devId, τη διεύθυνσή της dev address και το πιστοποιητικό της [devId, PK_dev]SK_reg. Πρέπει να σημειωθεί ότι στο πιστοποιητικό των συσκευών δεν αναφέρεται η διεύθυνσή τους. Έστω η συσκευή του χρήστη A με αναγνωριστικό devA και πιστοποιητικό [devA, PK_devA]SK_regA, ανακαλύπτει τη συσκευή του χρήστη B με αναγνωριστικό devB kai pistopoihtik'o [devB, PK_devB]SK_regB. Επαληθεύει ότι πρόκειται για συνεργαζόμενη συσκευή μέσα από κατάλληλο πρωτόκολλο που περιγράφεται στον παρακάτω ψευδοκώδικα.

Algorithm 3 devA: Establish trust with another device devB

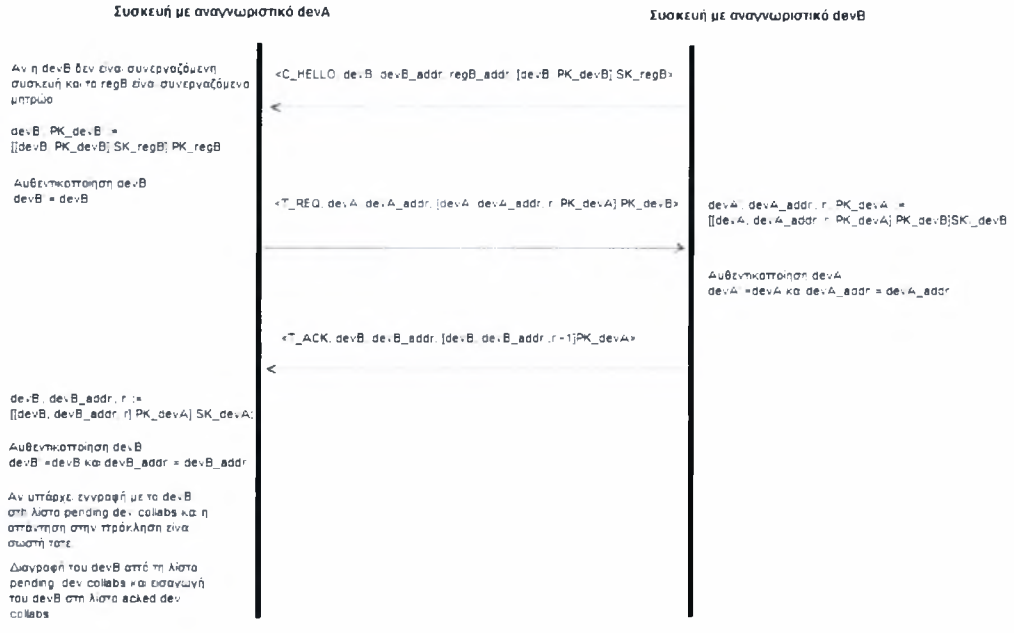
```
1: while (true) do
2:   m := get_next_msg();
3:   if (m = <C_HELLO,devB,devB_addr,regB_addr,
     [devB,PK_devB]SK_regB>) then
4:     if (!E <devB,*,*> in acked dev collabs) then
5:       if (E <regB_addr,PK_regB> in acked reg collabs) then
6:         devB',PK_devB' := [[devB,PK_devB]SK_regB]PK_regB
7:         if (devB' = devB) then
8:           if (!E <devB,r,t> in pending dev collabs or t<time()) then
9:             remove any entry <devB,*,*> from pending dev collabs
10:            r:= random()
11:            add entry <devB,r,time()+T> in pending dev collabs
12:            send_to(devB_addr,<T_REQ,devA,devA_addr,
               [devA,devA_addr,r,PK_devA]PK_devB>)
13:          end if
14:        end if
15:      end if
16:    end if
17:  else if (m = <T_REQ,devB,devB_addr,[devB,devB_addr,r,PK_devB]PK_-
     devA) then
18:    devB',devB_addr',r',PK_devB' := [[devB,devB_addr,r,PK_devB]PK_de-
       vA]SK_devA
19:    if (devB' = devB and devB_addr' = devB_addr) then
20:      send_to(devB_addr,<T_ACK,devA,devA_addr,
         [devA,devA_addr,r'+1]PK_devB>)
21:    end if
22:  else if (m = <T_ACK,devB,devB_addr,[devB,devB_addr,r]PK_devA> )
     then
23:    devB',devB_addr',r' := [[devB,devB_addr,r]PK_devA]SK_devA;
24:    if (devB' = devB and devB_addr' = devB_addr) then
25:      if (E <devB,r'-1,*> in pending dev collabs) then
26:        remove entry <devB,*,*> from pending dev collabs
27:        add entry <devB,devB_addr,PK_devB> in acked dev collabs
28:      end if
29:    end if
30:  end if
31: end while
```

Το παραπάνω πρωτόκολλο λειτουργεί ορθά ακόμα και όταν οι συσκευές ανήκουν στον ίδιο χρήστη και αυτό διότι όπως προαναφέρθηκε το αρχείο acked reg collabs που διαθέτουν οι συσκευές περιέχει και εγγραφή με τα στοιχεία του χρήστη στον οποίο ανήκουν.

Η συσκευή του χρήστη A με αναγνωριστικό devA λαμβάνει μήνυμα "heartbeat" από τη συσκευή του χρήστη B με αναγνωριστικό devB. Το μήνυμα αυτό περιλαμβάνει: 1) το αναγνωριστικό της συσκευής του χρήστη B (devB), 2) τη διεύθυνση της συσκευής του χρήστη B (devB_addr), 3) την IP διεύθυνση του μητρώου του χρήστη B (regB_addr), 4) το πιστοποιητικό της συσκευής του χρήστη B [devB, PK_devB]SK_regB. Σε περίπτωση που δεν υπάρχει ήδη εμπιστοσύνη με την συσκευή devB ελέγχεται αν υπάρχει συνεργασία μεταξύ του μητρώου του χρήστη A και του μητρώου του χρήστη B. Αν υπάρχει, η συσκευή devA ελέχγει τη γνησιότητα του πιστοποιητικού της συσκευής devB και εξάγει το δημόσιο κλειδί της αποκρυπτογραφώντας το κρυπτογραφημένο τμήμα του μηνύματος "heartbeat" με χρήση του δημοσίου κλειδιού του μητρώου regB, το οποίο είναι αποθηκευμένο στο αρχείο acked reg collabs. Στη συνέχεια ελέγχει αν η διεύθυνση του πιστοποιητικού ταιριάζει με αυτή του μηνυματος αυθεντικοποιώντας τη συσκευη devB. Αν η αυθεντικοποίηση της συσκευής devB γίνει με επιτυχία, γίνεται έλεγχος της λίστας με τις εκκρεμείς συνεργασίες (pending dev collabs). Σε περίπτωση που δεν εκκρεμεί συνεργασία με την συσκευή devB ή έχει περάσει χρόνος T απο τη στιγμή εισαγωγής της αίτησης στη λίστα pending dev collabs, εισάγεται καινούρια εγγραφή στη λιστα pending dev collabs. Η εγγραφή περιλαμβάνει 1) το αναγνωριστικό της συσκευής B (devB), 2) τυχαίο αριθμό , 3) την τρέχουσα χρονική στιγμη προσαυξημένη κατά χρονική σταθερά T. Επειτα στέλνει αίτηση συνεργασίας στη συσκευή devB. Το μήνυμα αίτησης συνεργασίας περιλαμβάνει: 1) το αναγνωριστικό της συσκευής του χρήστη A (devA), 2) τη διεύθυνση της συσκευής του χρήστη A (devA_addr), 3) κρυπτογραφημένα με το δημόσιο κλειδί της συσκευής devB τα: αναγνωριστικό της συσκευής του χρήστη A, τη διεύθυνση της συσκευής του χρήστη A, προκληση r, το δημόσιο κλειδί της συσκευής devA ([devA, devA_addr, r, PK_devA] PK_devB).

Η συσκευή devB λαμβάνει το μήνυμα αίτησης συνεργασίας και αποκρυπτογραφεί το κρυπτογραφημένο τμήμα με το ιδιωτικό κλειδί της. Ελέγχει αν το αναγνωριστικο και η διεύθυνση της συσκευής που στάλθηκαν είναι ίδια με αυτά του κρυπτογραφημένου τμήματος του μηνύματος, αυθεντικοποιώντας τη συσκευή devA. Αν η αυθεντικοποίηση πραγματοποιηθεί με επιτυχία, η συσκευή devB στέλνει μήνυμα επικύρωσης συνεργασίας στη συσκευή devA. Το μήνυμα περιλαμβάνει: 1) το αναγνωριστικό της συσκευής του χρήστη B (devB), 2) τη διεύθυνση της συσκευής του χρήστη B (devA_addr), 3) κρυπτογραφημένα με το δημόσιο κλειδί της συσκευής devA τα: αναγνωριστικό της συσκευής του χρήστη B, τη διεύθυνση της συσκευής του χρήστη B, απάντηση στην πρόκληση r ([devB, devB_addr, r+1] PK_devA).

Η συσκευή devA λαμβάνει το μήνυμα επικύρωσης συνεργασίας και αποκρυπτογραφεί το κρυπτογραφημένο τμήμα του μηνύματος με το ιδιωτικό κλειδί της. Ελέγχει αν το αναγνωριστικο και η διεύθυνση της συσκευής που στάλθηκαν είναι ίδια με αυτά του κρυπτογραφημένου τμήματος του μηνύματος, αυθεντικοποιώντας τη συσκευή devB. Αν η αυθεντικοποίηση γίνει με επιτυχία γίνεται έλεγχος για το αν υπάρχει εκκρεμής αίτηση συνεργασίας με την συσκευή devB. Ελέγχεται επίσης η ορθότητα της απάντησης στην πρόκληση. Αν οι παραπάνω έλεγχοι πραγματοποιηθούν με επιτυχία, η συσκευή devA τοποθετεί τη συσκευή devB στη λίστα με τις συσκευές με τις οποίες υπάρχει επικυρωμένη συνεργασία (acked dev collabs). Τέλος διαγράφει την συσκευή devB από την λίστα (pending dev collabs).



Σχήμα 3.4: Σύναψη συνεργασίας μεταξύ devA και devB

3.4 Ακύρωση συνεργασίας μεταξύ χρηστών - ενημέρωση των συσκευών

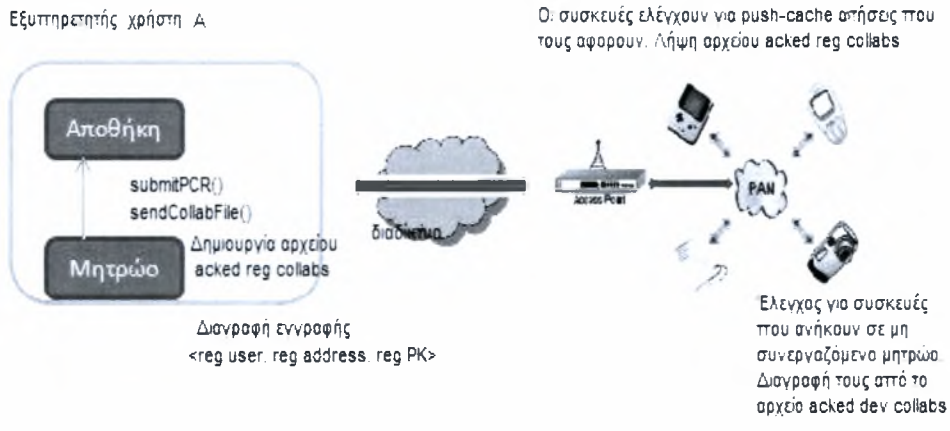
Σε περίπτωση που κάποιος χρήστης επιθυμεί να διακόψει κάποια συνεργασία μπορεί να το κάνει μέσω κατάλληλης διαδικτυακής εφαρμογής. Εκεί επιλέγει από τις ήδη υπάρχουσες συνεργασίες ποια επιθυμεί να διακόψει. Αποτέλεσμα της ενέργειάς του είναι η διαγραφή της αντίστοιχης εγγραφής από τη λίστα acked collabs. Στη συνέχεια δημιουργείται καινούριο αρχείο συνεργασιών, το οποίο αποστέλλεται στην

αποθήκη δεδομένων. Παράλληλα δημιουργούνται και αιτήσεις push-cache για το αρχείο συνεργασιών με προορισμό όλες τις συσκευές του χρήστη. Συνεπώς οι συσκευές κατά την περιοδική επικοινωνία τους με την αποθήκη, θα λάβουν το καινούριο αρχείο συνεργασιών.

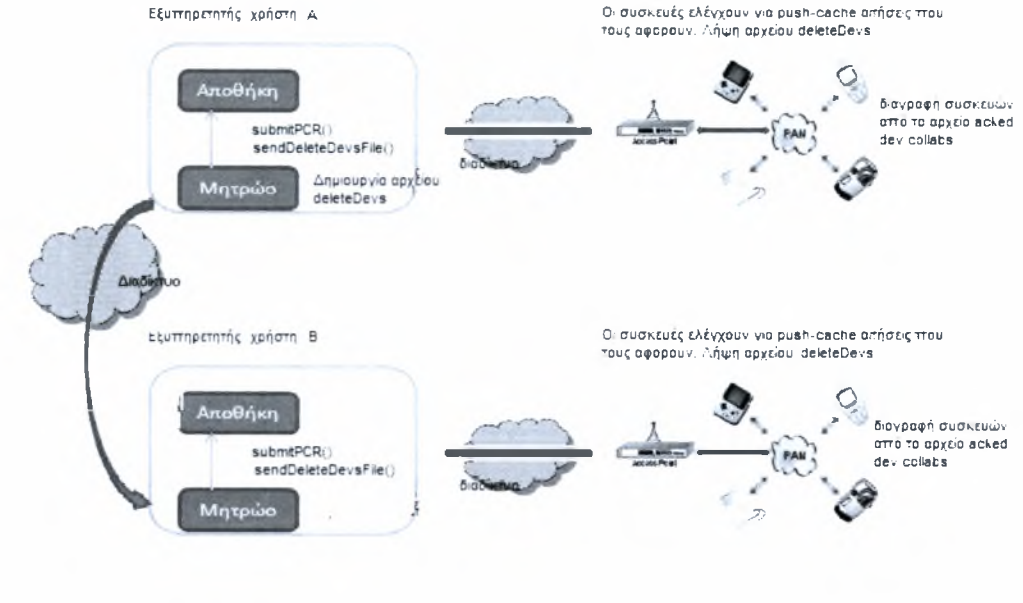
Τη στιγμή που γίνεται η λήψη του παραπάνω αρχείου, οι συσκευές ελέγχουν μήπως υπάρχει εμπιστοσύνη με κάποια συσκευή χρήστη , με τον οποίο δεν υπάρχει πλέον συνεργασία. Σε τέτοια περίπτωση η συσκευή διαγράφεται απο τη λίστα acked dev collabs.

Ειδική περίπτωση ακύρωσης συνεργασίας θεωρούμε την περίπτωση που οι συσκευές πρέπει να σταματήσουν να εμπιστεύονται μια συσκευή, η οποία ανήκει στον ίδιο χρήστη (π.χ λόγω κλοπής). Σε αυτήν την περίπτωση ο χρήστης διαγράφει τη συσκευή από το μητρώο του. Δημιουργεί ειδικό αρχείο με το αναγνωριστικό της συσκευής το οποίο αποστέλλει στην αποθήκη και για το οποίο δημιουργεί αίτηση push-cacheμε προορισμό όλες τις συσκευές του. Επιπρόσθετα με χρήση της βιβλιοθήκης μητρώου αποστέλλει το αρχείο αυτό σε όλα τα μητρώα με τα οποία συνεργάζεται. Αυτά με τη σειρά τους το αποστέλλουν στις αντίστοιχες αποθήκες και δημιουργούν αιτήσεις push-cahe με προορισμό το σύνολο των συσκευών τους.

Τελικά όλες οι συσκευές θα λάβουν το αρχείο με τις συσκευές προς διαγραφή, τις οποίες και διαγράφουν από το αρχείο acked dev collabs. Το αρχείο με τις συσκευές προς διαγραφή μετονομάζεται σε μαύρη λίστα, έτσι ώστε να αποφευχθεί επανασύναψη συνεργασίας με τη συσκευή.



Σχήμα 3.5: Ακύρωση συνεργασίας μεταξύ μητρώων



Σχήμα 3.6: Διαγραφή συσκεύης από μητρώο - ενημέρωση συνεργαζόμενων συσκευών

3.5 Αυθεντικοποίηση

Στο σύστημα OmniStore οι συσκευές προσφέρουν υπηρεσίες (π.χ το μητρώο παρέχει την υπηρεσία εγγραφής συσκευών). Οι υπηρεσίες αυτές ανακαλύπτονται μέσω ειδικού μηχανισμού ανακάλυψης υπηρεσιών που προσφέρει το σύστημα εκτέλεσης των συσκευών (runtime). Είναι απαραίτητο για κάθε συσκευή που επιθυμεί να χρησιμοποιήσει μια υπηρεσία να γνωρίζει αν απαιτείται αυθεντικοποίηση. Αυτό επιτυγχάνεται με τον παρακάτω μηχανισμό. Κατά τη διαφήμιση μιας υπηρεσίας, εκπέμπεται πληροφορία για τον τρόπο πρόσβασης σε αυτή. Συγκεκριμένα χρησιμοποιείται ένας ακέραιος που υποδηλώνει αν η υπηρεσία είναι δημόσια ή ιδιωτική. Την πληροφορία αυτή την αποθηκεύουν οι ενδιαφερόμενες για την υπηρεσία συσκευές. Συνεπώς όταν χρησιμοποιούν την υπηρεσία γνωρίζουν αν πρέπει να αυθεντικοποιηθούν ή όχι.

Ανάλογα με τον τύπο συσκευών που επικοινωνούν, διακρίνουμε τρεις περιπτώσεις αυθεντικοποίησης:

- κινητή συσκευή - κινητή συσκευή
- κινητή συσκευή - οντότητα υποδομής (π.χ συσκευή-μητρώο, συσκευή αποθήκη),
- οντότητα υποδομής - οντότητα υποδομής (π.χ μητρώο-αποθήκη)

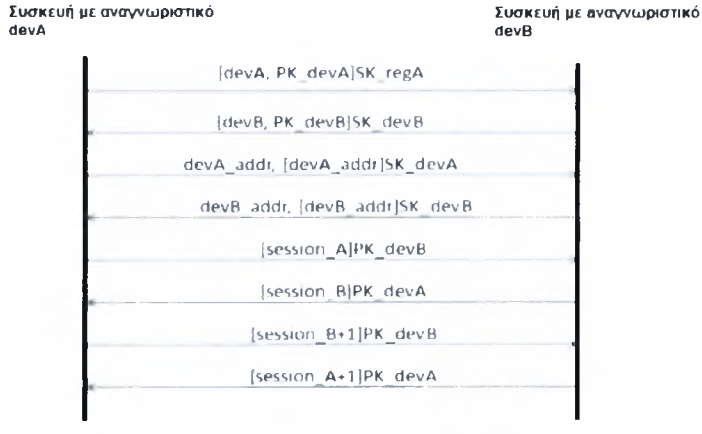
Όσον αφορά την πρώτη περίπτωση η αυθεντικοποίηση έχει λάβει ήδη χώρα κατά την εκτέλεση του πρωτοκόλλου σύναψης εμπιστοσύνης. Συνεπώς όταν μια κινητή συσκευή δεχθεί αίτηση αυθεντικοποίησης από μια άλλη κινητή συσκευή , απλά ελέγχει το αρχείο acked dev collabs . Αν το αναγνωριστικό της συσκευής βρεθεί στο αρχείο, η συσκευή αυθεντικοποιείται, αλλιώς η επικοινωνία διακόπτεται.

Όσον αφορά τις υπόλοιπες δύο περιπτώσεις (οι οποίες αναφέρονται σε συσκευές του ίδιου χρήστη) χρησιμοποιείται το παρακάτω πρωτόκολλο:

Algorithm 4 device authentication

1: {Πρώτη φάση:}
2: Αποστολή πιστοποιητικού [device_id,dev_PK]SK_reg
3: Λήψη απομακρυσμένου πιστοποιητικου [rem_device_id,rem_dev_PK]SK_reg
4: Αποκρυπτογράφηση πιστοποιητικου και εξαγωγή δημοσίου κλειδιού απομακρυσμένης οντότητας rem_dev_PK := [[rem_device_id,rem_dev_PK]SK_reg]PK_reg
5: Αποστολή της διεύθυνσης και της διεύθυνσης κρυπτογραφημένης με το ιδιωτικό κλειδί <device_addr,[device_addr]dev_SK>
6: Λήψη απομακρυσμένης διεύθυνσης και απομακρυσμένης κρυπτογραφημένης διεύθυνσης <rem_device_addr,[rem_device_addr]rem_dev_SK>
7: Αποκρυπτογράφηση απομακρυσμένης διεύθυνσης rem_token_device_addr := [[rem_device_addr]rem_dev_SK]rem_dev_PK
8: **if** (rem_device_addr != rem_token_device_addr) **then**
9: device failed to authenticate
10: **end if**
11: {Δεύτερη φάση: }
12: Παραγωγή αναγνωριστικού συνόδου session_id, κρυπτογράφηση με το δημόσιο κλειδί της απομακρυσμένης οντότητας [session_id]rem_dev_PK και αποστολή
13: Λήψη απομακρυσμένου αναγνωριστικού συνόδου [rem_session_id]dev_PK
14: session_id' := [[rem_session_id]dev_PK]dev_SK + 1 , αποστολή session_id'
15: Λήψη rem_session_id'
16: **if** (rem_session_id' != session_id -1) **then**
17: device failed to authenticate
18: **end if**
19: **return** rem_dev_PK

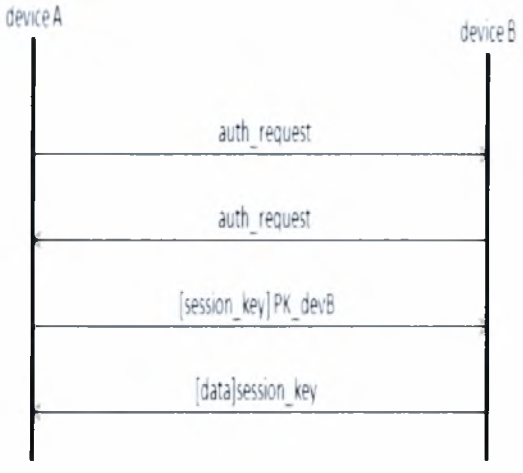
Σε πρώτη φάση οι οντότητες ανταλλάσουν τα ψηφιακά πιστοποιητικά τους, τα αποκρυπτογράφούν με το δημόσιο κλειδί του μητρώου τους και εξάγουν το δημοσίο κλειδί της απομακρυσμένης οντότητας. Στη συνέχεια οι οντότητες χρησιμοποιούν το ιδιωτικό κλειδί τους για να υπογράψουν τις διευθύνσεις τους. Έπειτα κάθε οντότητα στέλνει τη διεύθυνση της τόσο κρυπτογραφημένη όσο και μη κρυπτογραφημένη. Κάθε οντότητα αποκρυπτογραφεί την κρυπτογραφημένη διεύθυνση με χρήση του δημοσίου κλειδιού της απομακρυσμένης οντότητας (εξαγωγή από το πιστοποιητικό). Αν οι αποκρυπτογραφημένες διευθύνσεις είναι ίδιες με τις μη - κρυπτογραφημένες, περνάμε στη δεύτερη φάση, όπου προκαλούμε την απομακρυσμένη οντότητα να χρησιμοποιήσει το ιδιωτικό κλεδί της, υπογράφοντας αναγνωριστικό συνόδου, το οποίο επαληθεύεται με το δημόσιο κλειδί της που εξάγαμε από το πιστοποιητικό. Αποφεύγεται έτσι η επανεκπομπή του πιστοποιητικού.



Σχήμα 3.7: Αυθεντικοποίηση κινητής συσκευής/συσκευής υποδομής - συσκευής υποδομής

3.6 Εμπιστευτικότητα

Όσον αφορά την εμπιστευτικότητα δεδομένων εξασφαλίζεται με χρήση κρυπτογραφικών τεχνικών. Όταν μια οντότητα επιθυμεί να στείλει ευαίσθητα δεδομένα σε μια άλλη, αρχικά αυθεντικοποιείται. Στη συνέχεια χρησιμοποιεί το δημόσιο κλειδί της απομακρυσμένης οντότητας (επιστρέφεται από τον αλγόριθμο αυθεντικοποίησης) για να κρυπτογραφήσει ένα συμμετρικό κλειδί το οποίο χρησιμοποιείται στην περαιτέρω επικοινωνία.



Σχήμα 3.8: Επικοινωνία οντοτήτων

3.7 Σύνοψη

Σε αυτό το κεφάλαιο αναπτύξαμε ένα μηχανισμό ασφαλούς συνεργασίας κινητών συσκευών διαφορετικών χρηστών, επεκτείνοντας το σύστημα OmniStore. Ο μηχανισμός περιλαμβάνει τα έξι βήματα της διαδικασίας ισχυρής αυθεντικοποίησης σε δίκτυα κινητής υπολογιστικής (κεφάλαιο 2).

Θα συνοψίσουμε παραθέτοντας τις ενέργειες που γίνονται σε κάθε βήμα της διαδικασίας ισχυρής αυθεντικοποίησης και τέλος θα κάνουμε μια αξιολόγηση του συστήματος, βάσει των έξι απαιτήσεων αυθεντικοποίησης σε συστήματα κινητής υπολογιστικής (κεφάλαιο 2).

- **βήμα 1: bootstrapping:** Οι κινητές συσκευές κάθε χρήστη προμηθεύονται το ψηφιακό πιστοποιητικό τους κατά την εγγραφή τους στο μητρώο.
- **βήμα 2: προ-αυθεντικοποίηση:** Δημιουργία συνεργασίας μεταξύ των μητρώων των χρηστών,ανταλλαγή δημοσίων κλειδιών των μητρώων δημιουργία του αρχείου acked reg collabs (Algorithm 2).
- **βήμα 3: Δημιουργία διαπιστευτηρίων:** Δημιουργία εμπιστοσύνης μεταξύ κινητών συσκευών , ανταλλαγή των δημοσίων κλειδιών τους, δημιουργία αρχείου acked dev collabs (Algorithm 3).
- **βήμα 4: Αυθεντικοποίηση:** Ουσιατικά επιτυγχάνεται μέσω του πρωτοκόλλου δημιουργίας εμπιστοσύνης μεταξύ κινητών συσκευών. Τυπικά επιτυγχάνεται με τον έλεγχο ύπαρξης της διεύθυνσης και του αναγνωριστικού της συσκευής που επιθυμεί να αυθεντικοποιηθεί, στο αρχείο acked dev collabs.
- **βήμα 5: Έλεγχος:** Δεν υπάρχει κάποιος μηχανισμός ελέγχου κακής συμπεριφοράς των συσκευών. Ο χρήστης ελέγχει αν κάποια συσκευή του χάθηκε/εκλάπη.
- **βήμα 6: Ανάκληση:** Ο χρήστης μπορεί να διακόψει κάθε συνεργασία με οποιοδήποτε μητρώο με αποτέλεσμα να διακόπτεται η εμπιστοσύνη και μεταξύ των αντίστοιχων κινητών συσκευών. Επιπλέον υποστηρίζεται η ανάκληση των διαπιστευτηρίων από κάποια συγκεκριμμένη συσκευή και η ενημέρωση όλων των συσκευών (ίδιου/διαφορετικών χρηστών) για το παραπάνω γεγονός.

Ο παρακάτω πίνακας παρουσιάζει την αξιολόγηση του συστήματος με βάση της απαιτήσεις.

Πίνακας 3.1: Ανάλυση απαιτήσεων ισχυρής αυθεντικοποίησης

Απαιτήσεις	Ανάλυση
1) Ισχυρή αυθεντικοποίηση	Χρήση ασύμμετρης κρυπτογραφίας (κλειδιά RSA) και ψηφιακών πιστοποιητικών. Χρήση συμμετρικής κρυπτογραφίας (κλειδιά DES)
2) Ευκολία στη χρήση	Δεν απαιτείται καμία αλληλεπίδραση συσκευής χρήστη
3) Κλιμάκωση	Δεν αναμένεται μεγάλος αριθμός χρηστών/συσκευών. Δεν υπάρχει κάποιο κεντρικό σημείο συμφόρησης.
4) Μικρός φόρτος	Η αυθεντικοποίηση συσκευών λαμβάνει χώρα μόνο όταν αυτές συναντηθούν για πρώτη φορά, οπότε δεν υπάρχει μεγάλο κόστος επικοινωνίας.
5) Υποστήριξη ανάκλησης	Ο χρήστης ακυρώνει οποιαδήποτε συνεργασία, και διαγράφει οποιαδήποτε συσκευή. Οι υπόλοιπες συσκευές (όλων των χρηστών) ενημερώνονται ανάλογα.
6) Διαλειτουργικότητα	Η αυθεντικοποίηση, μέσω του πρωτοκόλλου ανάπτυξης εμπιστοσύνης μεταξύ των συσκευών γίνεται με τον ίδιο τρόπο ανάμεσα σε συσκευές τόσο του ίδιου χρήστη όσο και διαφορετικών.

Κεφάλαιο 4

Συναφείς εργασίες

Σε αυτήν την ενότητα κάνουμε μια αναφορά σε συστήματα ασφαλούς συνεργασίας κινητών συσκευών. Θα γίνει επίσης προσπάθεια εντοπισμού κοινών σημείων και διαφορών με την προσέγγιση μας.

4.1 UPnP (Universal Plug and play) προδιαγραφή ασφάλειας

Το UPnP επιτρέπει τη δημιουργία ομότιμων δικτύων που αποτελούνται από προσωπικούς υπολογιστες, συσκευές με ικανότητα δικτύωσης και ασύρματες συσκευές. Βασίζεται σε καθιερωμένα πρότυπα όπως TCP/IP, UDP, HTTP, XML. Υποστηρίζει δικτύωση με "μηδενική διαμόρφωση" (zero - configuration). Κάθε συμβατή UPnP συσκευή από οποιονδήποτε κατασκευαστή μπορεί να εισέλθει δυναμικά σε ένα δίκτυο, να αποκτήσει IP διεύθυνση και να ανακοινώσει το όνομά της. Επιπλέον μπορεί να ανακοινώσει τις δυνατότητές της και να λάβει πληροφορία για τις δυνατότητες άλλων συσκευών. Το UPnp αποτελείται από συσκευές και σημεία ελέγχου. Οι συσκευές διαφημίζουν την παρουσία τους μέσω πρωτοκόλλου ανακάλυψης και υπηρεσίες που προσφέρουν: συλλογές ενεργειών SOAP που λαμβάνουν τα σημεία ελέγχου. Η ασφάλεια UPnP [4] ασχολείται με το πρωτόκολλο ελέγχου, SOAP. Αφαλίζει τα μηνύματα ελέγχου SOAP και τις απαντήσεις σε αυτά. Η ασφάλεια των μηνυμάτων περιλαμβάνει: αναγνώριση, ακεραιότητα, αυθεντικοποίηση, φρεσκάδα, εξουσιοδότηση, μυστικότητα.

Ο αποστολέας του μηνύματος αναγνωρίζεται από το αναγνωριστικό ασφάλειας (SecurityId), το οποίο προκύπτει από εφαρμογή συνάρτησης κατακερματισμού στο δημόσιο κλειδί της συσκευής. Η ροή ασφάλειας των μηνυμάτων ελέγχου είναι η εξής:

1. Λαμβάνεται ένα μήνυμα και αναλύεται. Αν περιλαμβάνεται <SecurityInfo> στην SOAP κεφαλίδα το μηνυμα θεωρείται υπογεγραμμένο.

2. Αν το μήνυμα δεν είναι υπογεγραμμένο, ο ιδιοκτήτης του θέτεται "άγνωστος " και προχωρούμε στον έλεγχο εξουσιοδότησης.

3. Αν το μήνυμα είναι υπογεγραμμένο γίνεται επαλήθευση της υπογραφής και της φρεσκάδας. Η επαλήθευση της υπογραφής επαληθεύει τόσο την ακεραιότητα του μηνύματος όσο και την αυθεντικότητα της προέλευσης.

4. Αν η υπογραφή είναι ορθή και το μήνυμα φρέσκο, τότε ο ιδιοκτήτης του θέτεται "SecurityId". Αλλιώς το μήνυμα αποτυγχάνει και παράγεται μήνυμα σφάλματος.

5. Αν το μήνυμα πρέπει να εξεταστεί για εξουσιοδότηση, συλλέγονται οι εξής πληροφορίες: λίστα ιδιοκτητών, λίστα ελέγχου πρόσβασης, τοπικά αποθηκευμένα πιστοποιητικά και πιστοποιητικά που παρέχονται στο στοιχείο <KeyInfo> του μηνύματος. Λαμβάνεται το όνομα της ενέργειας του μηνύματος και χρησιμοποιείται για να βρεθεί η άδεια που πρέπει να έχει ο χρήστης προκειμένου να εκτελέσει αυτήν την ενέργεια. Στη συνέχεια ελέγχονται οι πληροφορίες εξουσιοδότησης για να διαπιστωθεί αν ο χρήστης έχει την απαιτούμενη άδεια για να εκτελέσει την ενέργεια.

6. Αν ο χρήστης δεν είναι εξουσιοδοτημένος το μήνυμα αποτυγχάνει και παράγεται μήνυμα σφάλματος. Αν ο χρήστης είναι εξουσιοδοτημένος εκτελείται η επιθυμητή ενέργεια.

Το παραπάνω σύστημα δεν παρουσιάζει ομοιότητες με την προσέγγιση μας. Η διαφορά που αξίζει να σημειωθεί είναι ότι η ασφάλεια επιτυγχάνεται μέσω ειδικής συσκευής με όνομα "SecurityConsole", η οποία πρέπει να ανακαλύψει με πολύπλοκο ασφαλή τρόπο την συσκευή του χρήστη (μέσω τροποποιημένου μηχανισμού ανακάλυψης). Στο σύστημα μας υπεύθυνες για την ασφάλεια είναι οι ίδιες οι συσκευές.

4.2 Bluetooth

Μια Bluetooth συσκευή μπορεί να απαιτήσει αυθεντικοποιημένη επικοινωνία για κάποια υπηρεσία που παρέχει. Η αυθεντικοποίηση bluetooth [1] γίνεται με χρήση κωδικών PIN . Ο χρήστης πρέπει να τοποθετήσει τον ίδιο κωδικό PIN και στις δύο συσκευές. Μόλις τοποθετηθούν οι κωδικοι παράγεται ένα κλειδί συνδεσμου (link key). Οι συσκευές αποθηκεύουν αυτό το κλειδί και το χρησιμοποιούν για να αυθεντικοποιηθουν. Η διαδικασία αυτή ονομάζεται ταίριασμα.

Κύρια ομοιότητα της προσέγγισης μας σε σχέση με τη διαδικασία αυθεντικοποίησης bluetooth είναι ότι αυτή είναι προαιρετική. Όσον αφορά το μηχανισμο αυθεντικοποίησης, όπως είδαμε στο bluetooth χρησιμοποιείται συμμετρική κρυπτογραφία, ενώ στο σύστημα μας ασύμμετρη. Θερούμε βασικό μειονέκτημα της αυθεντικοποίησης bluetooth την εισαγωγή κωδικού και στις δύο συσκευές, κάτι που σημαίνει αλληλεπίδραση με το χρήστη.

4.3 inter - device authentication framework

Στο πλαίσιο αυθεντικοποίησης συσκευών που περιγράφεται στην δημοσίευση [6] προτείνεται ένας μηχανισμός ασφαλούς επικοινωνίας μεταξύ κινητών συσκευών. Αρχικά ο χρήστης γίνεται ιδιοκτήτης της συσκευής. Στη συνέχεια ακολουθεί η αυθεντικοποίηση συσκευών και ο έλεγχος πρόσβασης. Κάθε συσκευή διαθέτει ψηφιακό πιστοποιητικό X.509 , ιδιωτικό/δημόσιο κλειδί και λίστα με τις αρχές πιστοποίησης (ΑΠ) που εμπιστεύεται. Όλα τα παραπάνω παρέχονται από τον κατασκευαστή. Η συσκευή που επιθυμεί να αυθεντικοποιηθεί στέλνει το πιστοποιητικό της. Γίνεται επαλήθευση του πιστοποιητικού με χρήση της λίστας ΑΠ που εμπιστεύεται συσκευή που δέχεται τη σύνδεση. Αν η επαλήθευση γίνει με επιτυχία τότε η συσκευή που δέχεται τη σύνδεση στέλνει πρόκληση στη συσκευή που επιθυμεί να αυθεντικοποιηθεί. Αυτή παράγει ψηφιακή υπογραφή με χρήση της πρόκλησης και του ιδιωτικού κλειδιού της και την επιστρέφει. Στη συνέχεια γίνεται επαλήθευση της ψηφιακής υπογραφής και η διαδικασία αυθεντικοποίησης ολοκληρώνεται. Για αμοιβαία αυθεντικοποίηση απαιτείται η ίδια διαδικασία στην αντίστροφη κατεύθυνση.

Βασική ομοιότητα του παραπάνω πλαισίου και της προσέγγισης μας είναι ότι γίνεται χρήση ψηφιακών πιστοποιητικών και λίστας ΑΠ που εμπιστεύεται κάθε συσκευή. Υπενθυμίζουμε ότι στην προσέγγιση μας τα μητρώα λειτουργούν και σαν ΑΠ, οπότε η λίστα με τα μητρώα, με τα οποία υπάρχει εμπιστοσύνη (acked reg collabs), είναι στην ουσία μια λίστα με ΑΠ. Βασική διαφορά μεταξύ των δύο συστημάτων είναι ότι στην προσέγγισή μας απαιτείται αυθεντικοποίηση συσκευών μόνο την πρώτη φορά που αυτές θα συναντηθούν, ενώ στο εν λόγω πλαίσιο κάθε φορά που οι συσκευές έρχονται σε επαφή.

Βιβλιογραφία

[1] bluetooth sig: Specifications of the bluetooth system version 2.0 + edr, 2004. [cited at p. 38]

[2] *Authentication protocols for ad hoc networks: Taxonomy and research issues, Proceedings of the 1st ACM international workshop on Quality of service and security in wireless and mobile networks*, October 2005. [cited at p. 17]

[3] Alexandros Karypidis. *Omnistore: Mechanisms for automating data management in a personal system comprising several portable devices, PHD thesis.* PhD thesis, November 2006. [cited at p. 3]

[4] Carl Ellison. upnp security ceremonies, October 2003. [cited at p. 37]

[5] Connie Chang Helen Tang, Mazda Salmanian. *Strong authentication for tactical Mobile Ad Hoc Networks, technical memorandum*, July 2007. [cited at p. 16]

[6] Manabu Hirano, Takeshi Okuda, and Suguru Yamaguchi. design and implementation of an inter-device authentication framework guaranteeing explicit ownership. *IPSJ Digital Courier*, February 2008. [cited at p. 39]

[7] Yang Xiao. *Security in distributed, grid, mobile and pervasive computing.* 2007. [cited at p. 15]

Κατάλογος Σχημάτων

Κατάλογος Πινάκων